



OFFICIAL MICROSOFT LEARNING PRODUCT

10964C

**10964C: Cloud and Datacenter Monitoring
with System Center Operations Manager**

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2014 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at

<http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners

Product Number: 10964C

Part Number (if applicable): X19-43316

Released: 09/2014

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

**BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS.
IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.**

If you comply with these license terms, you have the rights below for each license you acquire.

1. DEFINITIONS.

- a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
- b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
- c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
- d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.
- e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
- f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
- g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.
- h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.
- i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
- j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.
- k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

- I. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
 - m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
 - n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.
 - o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.
- 2. USE RIGHTS.** The Licensed Content is licensed not sold. The Licensed Content is licensed on a ***one copy per user basis***, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

a. **If you are a Microsoft IT Academy Program Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
 - 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 - 2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 - 3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,
- provided you comply with the following:
 - iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 - iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
 - v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
 - vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

- vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
- viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
- ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. **If you are a Microsoft Learning Competency Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
 2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

provided you comply with the following:

- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
- v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
- vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
- viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
- ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- x. you will only provide access to the Trainer Content to Trainers.

c. **If you are a MPN Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
 - ii. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,
- provided you comply with the following:**
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 - iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
 - v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
 - vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
 - vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
 - viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
 - ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
 - x. you will only provide access to the Trainer Content to Trainers.

d. **If you are an End User:**

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

e. **If you are a Trainer.**

- i. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

- ii. You may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "customize" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

2.2 Separation of Components. The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.

2.3 Redistribution of Licensed Content. Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.

2.4 Third Party Notices. The Licensed Content may include third party code tent that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code ntent are included for your information only.

2.5 Additional Terms. Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY. If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("Pre-release"), then in addition to the other provisions in this agreement, these terms also apply:

- a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.
- b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
- c. **Pre-release Term.** If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("Pre-release term"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

- 4. SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
 - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
 - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
 - modify or create a derivative work of any Licensed Content,
 - publicly display, or make the Licensed Content available for others to access or use,
 - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
 - work around any technical limitations in the Licensed Content, or
 - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.
- 5. RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.
- 6. EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
- 7. SUPPORT SERVICES.** Because the Licensed Content is "as is", we may not provide support services for it.
- 8. TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
- 9. LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
- 10. ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
- 11. APPLICABLE LAW.**
 - a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

- b. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.
- 12. LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
- 13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
- 14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US\$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised July 2013

Welcome!

Thank you for taking our training! We've worked together with our Microsoft Certified Partners for Learning Solutions and our Microsoft IT Academies to bring you a world-class learning experience—whether you're a professional looking to advance your skills or a student preparing for a career in IT.

- **Microsoft Certified Trainers and Instructors**—Your instructor is a technical and instructional expert who meets ongoing certification requirements. And, if instructors are delivering training at one of our Certified Partners for Learning Solutions, they are also evaluated throughout the year by students and by Microsoft.
- **Certification Exam Benefits**—After training, consider taking a Microsoft Certification exam. Microsoft Certifications validate your skills on Microsoft technologies and can help differentiate you when finding a job or boosting your career. In fact, independent research by IDC concluded that 75% of managers believe certifications are important to team performance¹. Ask your instructor about Microsoft Certification exam promotions and discounts that may be available to you.
- **Customer Satisfaction Guarantee**—Our Certified Partners for Learning Solutions offer a satisfaction guarantee and we hold them accountable for it. At the end of class, please complete an evaluation of today's experience. We value your feedback!

We wish you a great learning experience and ongoing success in your career!

Sincerely,

Microsoft Learning
www.microsoft.com/learning



¹ IDC, Value of Certification: Team Certification and Organizational Performance, November 2006

Acknowledgements

Microsoft Learning would like to acknowledge and thank the following for their contribution towards developing this title. Their effort at various stages in the development has ensured that you have a good classroom experience.

Gordon McKenna – Content Developer

Gordon is a Microsoft System Center Cloud and Datacenter Management Most Valuable Professional (MVP) with over 15 years of experience, and is an expert in Microsoft management technologies. Currently, Gordon helps run the U.K.'s leading System Center consultancy, Inframon, and was personally involved with some of the largest System Center implementations in EMEA. Gordon is a well-known speaker on System Center and regularly appears at TechEd in the U.K. and the U.S. He is also a regular speaker at MMS, WPC, and many partner and community events.

Sean Roberts – Content Developer

Sean (MCTS, Bbus) is a joint owner of Inframon Ltd, a U.K.-based System Center consultancy. Originally from a development background, Sean has over 15 years of experience designing business intelligence solutions for many Fortune 500 companies. For seven years, he focused on building System Center-based operational reports and dashboards to help organizations measure, trend, and score their IT capabilities.

Justin Kimber – Content Developer

Justin (MCTS, MCITP, MCSA, MCSE, MCP) has worked in the IT industry for over 17 years in various systems management roles. For six years, he worked as technical director at Inframon, Ltd. In this role, he was responsible for designing and implementing some of the largest systems management roll-outs in EMEA. He was personally involved with the roll-out of a global, application monitoring platform for Microsoft IT.

Contents

Module 1: Overview and Architecture

Module Overview	1-1
Lesson 1: Overview of Operations Manager	1-2
Lesson 2: Overview of Key Features in Operations Manager	1-7
Lesson 3: Overview of Core Components and Topology	1-11
Lesson 4: Addressing Cloud and Datacenter Issues by Using Operations Manager	1-16
Lesson 5: Planning and Sizing System Center 2012 R2 Operations Manager	1-19
Lab: Using the System Center 2012 Operations Manager Sizing Helper Tool	1-27
Module Review and Takeaways	1-33

Module 2: Deploying a New System Center 2012 R2 Operations Manager Management Group

Module Overview	2-1
Lesson 1: Overview of Security Considerations	2-3
Lesson 2: Designing the Management Group	2-6
Lesson 3: Installing System Center 2012 R2 Operations Manager	2-11
Lesson 4: Configuring Operations Manager Default Settings	2-17
Lesson 5: Deploying the Operations Manager Agent	2-21
Lesson 6: Configuring Agentless Exception Monitoring (AEM)	2-30
Lesson 7: Configuring Audit Collection Services	2-34
Lab: Installing System Center 2012 R2 Operations Manager and Deploying Agents	2-40
Module Review and Takeaways	2-63

Module 3: Upgrading Operations Manager

Module Overview	3-1
Lesson 1: Guidelines for Migration and Upgrade to System Center 2012 R2 Operations Manager	3-2
Lesson 2: Upgrading to System Center 2012 R2 Operations Manager	3-5
Lesson 3: Migrating to System Center 2012 R2 Operations Manager	3-14
Lab: Upgrading to System Center 2012 R2 Operations Manager	3-16
Module Review and Takeaways	3-30

Module 4: Configuring Fabric and Application Monitoring

Module Overview	4-1
Lesson 1: Introduction to Management Packs	4-2
Lesson 2: Configuring Application Monitoring	4-17
Lesson 3: Configuring Network Device Monitoring	4-30
Lesson 4: Configuring Fabric Monitoring	4-36
Lab: Configuring Application and Fabric Monitoring	4-47
Module Review and Takeaways	4-65

Module 5: Application Performance Monitoring

Module Overview	5-1
Lesson 1: Application Performance Monitoring	5-2
Lesson 2: Using IntelliTrace	5-18
Lesson 3: Team Foundation Server Integration	5-23
Lab: Monitoring .NET Framework Applications	5-26
Module Review and Takeaways	5-38

Module 6: End to End Service Monitoring

Module Overview	6-1
Lesson 1: Management Pack Templates	6-2
Lesson 2: Distributed Application Models	6-18
Lesson 3: Global Service Monitor	6-27
Lesson 4: Real-Time Visio Dashboards	6-33
Lab: Configuring End-to-End Service Monitoring	6-38
Module Review and Takeaways	6-52

Module 7: Scorecards, Dashboards, and Reporting

Module Overview	7-1
Lesson 1: Configuring and Managing Reporting in Operations Manager	7-3
Lesson 2: Configuring Service Level Tracking	7-10
Lesson 3: Configuring the Operations Manager SharePoint Web Part	7-13
Lesson 4: Dashboards and Widgets	7-16
Lesson 5: Creating Custom Dashboards	7-23
Lab: Configuring Reporting, Dashboards, and Service Level Tracking	7-27

Module Review and Takeaways	7-47
-----------------------------	-------------

Module 8: Configuring and Customizing the Operations Console

Module Overview	8-1
Lesson 1: Security, Scoping, and User Roles	8-2
Lesson 2: Creating Custom Views and Alert Resolution States	8-7
Lesson 3: Configuring Notification Subscriptions	8-12
Lesson 4: Creating Diagnostic and Recovery Tasks	8-17
Lab: Customizing the Operations Console	8-22
Module Review and Takeaways	8-38

Module 9: Management Pack Authoring

Module Overview	9-1
Lesson 1: Management Pack Authoring Concepts	9-2
Lesson 2: Authoring Management Packs by Using the Operations Console	9-9
Lesson 3: Authoring Management Packs by using the Visual Studio Authoring Extensions	9-19
Lab: Authoring Management Packs	9-35
Module Review and Takeaways	9-61

Module 10: Integrating Operations Manager with Other System Center Components

Module Overview	10-1
Lesson 1: Service Manager Integration	10-2
Lesson 2: Data Protection Manager Integration	10-10
Lesson 3: Orchestrator Integration	10-16
Lab: Configuring System Center Integration	10-25
Module Review and Takeaways	10-35

Module 11: Troubleshooting, Tuning, and Disaster Recovery

Module Overview	11-1
Lesson 1: Troubleshooting and Maintaining Operations Manager Core	
Components	11-3
Lesson 2: Tuning Management Packs	11-18
Lesson 3: Configuring SQL AlwaysOn for Operations Manager	11-24
Lesson 4: Configuring Data Retention in Operations Manager	11-28
Lesson 5: Disaster Recovery in Operations Manager	11-34
Lab: Troubleshooting Operations Manager	11-42
Module Review and Takeaways	11-44

Lab Answer Keys

Module 1 Lab: Using the System Center 2012 Operations Manager	
Sizing Helper Tool	L01-1
Module 2 Lab: Installing System Center 2012 R2 Operations Manager	
and Deploying Agents	L02-1
Module 3 Lab: Upgrading to System Center 2012 R2 Operations Manager	L03-1
Module 4 Lab: Configuring Application and Fabric Monitoring	L04-1
Module 5 Lab: Monitoring .NET Framework Applications	L05-1
Module 6 Lab: Configuring End-to-End Service Monitoring	L06-1
Module 7 Lab: Configuring Reporting, Dashboards, and Service	
Level Tracking	L07-1
Module 8 Lab: Customizing the Operations Console	L08-1
Module 9 Lab: Authoring Management Packs	L09-1
Module 10 Lab: Configuring System Center Integration	L10-1
Module 11 Lab: Troubleshooting Operations Manager	L11-1

About This Course

This section provides a brief description of the course, audience, suggested prerequisites, and course objectives.

Course Description

Before implementing Microsoft System Center 2012 R2 Operations Manager, it is important to understand the key features and functionality that it provides. This will help you understand how Operations Manager can be used to solve many common problems that arise in the cloud or datacenter, such as ensuring service levels are maintained and that critical line-of-business applications are available and performing at optimum levels.

Operations Manager is a comprehensive monitoring solution that requires careful planning before it is deployed into any IT environment. You must understand the hardware and software requirements of the solution and any security implications, such as those associated with monitoring computers in a trust boundary, perimeter network, or public cloud. When you configure the storage for the Operations Manager databases, you should have a good understanding of the number of computers and devices that are monitored to appropriately size the databases.

This module introduces students to the components contained in an Operations Manager Management Group and describes the dependency and relationships between the various components. Students will be shown how to plan for and design an Operations Manager Management Group.

Audience

This course is intended for cloud and datacenter administrators who are new to System Center 2012 R2 Operations Manager and are responsible for deploying, configuring and operating it in their cloud or datacenter.

Student Prerequisites

In addition to their professional experience, students who attend this training should already have the following technical knowledge:

- One or more years' experience in the design and implementation of System Center Operations 2007 R2 or System Center 2012 Operations Manager is desired.
- Working knowledge of Windows Server 2008 R2 and Windows Server 2012 R2.
- Working knowledge of SQL Server 2008 R2 and SQL Server 2012.

Course Objectives

After they complete this course, students will be able to do the following:

- Plan for the deployment of System Center 2012 R2 Operations Manager including:
 - Defining hardware and software requirements.
 - Describing security considerations.
 - Architect a highly available System Center and Microsoft SQL Server platform utilizing Microsoft SQL Server AlwaysOn.
 - Planning for migration and upgrade scenarios to System Center 2012 R2 Operations Manager.
- Customize the Operations Console with User Roles.
- Perform different methods of Agent deployment with System Center 2012 R2 Operations Manager.

- Implement key Management Pack concepts and elements including Management Packs Templates.
- Configure Notifications, Reporting, and Service Level Tracking in System Center 2012 R2 Operations Manager.
- Configure the following:
 - Audit Collection Services.
 - Agentless Exception Monitoring.
 - Operations Manager SharePoint Web Part in System Center 2012 R2 Operations Manager.
- Configure Application Performance Monitoring and Network Device monitoring in System Center 2012 R2 Operations Manager.
- Configure dashboards and widgets in System Center 2012 R2 Operations Manager.
- Describe how to use new cloud-based features including System Center Global Service Monitor and System Center Advisor.
- Configure integration between System Center 2012 R2 Operations Manager and other System Center 2012 R2 components.
- Troubleshoot an Operations Manager Management Group.
- Perform disaster recovery in System Center 2012 R2 Operations Manager.

There is no direct mapping to any certification exam.

Course Outline

The course outline is as follows:

Module 1, "Overview and Architecture"

Module 2, "Deploying Operations Manager"

Module 3, "Upgrading Operations Manager"

Module 4, "Configuring Fabric and Application Monitoring"

Module 5, "Application Performance Monitoring"

Module 6, "End to End Service Monitoring"

Module 7, "Scorecards, Dashboards and Reporting"

Module 8, "Configuring and Customizing the Console"

Module 9, "Management Pack Authoring"

Module 10, "System Center Integration"

Module 11, "Troubleshooting, Tuning and Disaster Recovery"

Course Materials

The following materials are included with your kit:

Course Handbook: a succinct classroom learning guide that provides the critical technical information in a crisp, tightly-focused format, which is essential for an effective in-class learning experience. You may be accessing either a printed course hand book or digital courseware material via the Arvato Skillpipe reader. Your Microsoft Certified Trainer will provide specific details but both contain the following:

- **Lessons:** guide you through the learning objectives and provide the key points that are critical to the success of the in-class learning experience.
- **Labs:** provide a real-world, hands-on platform for you to apply the knowledge and skills learned in the module.
- **Module Reviews and Takeaways:** provide on-the-job reference material to boost knowledge and skills retention.
- **Lab Answer Keys:** provide step-by-step lab solution guidance.



Additional Reading: Course Companion Content on the <http://www.microsoft.com/learning/en/us/companion-moc.aspx> Site: searchable, easy-to-browse digital content with integrated premium online resources that supplement the Course Handbook.

- **Modules:** include companion content, such as questions and answers, detailed demo steps and additional reading links, for each lesson. Additionally, they include Lab Review questions and answers and Module Reviews and Takeaways sections, which contain the review questions and answers, best practices, common issues and troubleshooting tips with answers, and real-world issues and scenarios with answers.
- **Resources:** include well-categorized additional resources that give you immediate access to the most current premium content on TechNet, MSDN®, or Microsoft® Press®.



Additional Reading: Student Course files on the <http://www.microsoft.com/learning/en/us/companion-moc.aspx> Site: includes the Allfiles.exe, a self-extracting executable file that contains all required files for the labs and demonstrations.

- **Course evaluation:** at the end of the course, you will have the opportunity to complete an online evaluation to provide feedback on the course, training facility, and instructor.
- To provide additional comments or feedback on the course, send an email to support@mscourseware.com. To inquire about the Microsoft Certification Program, send an email to mcphelp@microsoft.com.

Virtual Machine Environment

This section provides the information for setting up the classroom environment to support the business scenario of the course.

Virtual Machine Configuration

In this course, you will use virtual machines built in Microsoft® Hyper-V to perform the labs.

 **Note:** At the end of each lab, you may need to revert the virtual machines to a previous checkpoint. You can find the instructions for this procedure at the end of each lab

The following table shows the role of each virtual machine that is used in this course:

Virtual machine	Role
LON-DC1	Windows Server 2012 R2 Domain Controller.
LON-AP1	Windows Server 2012 server running SharePoint Server 2013.
LON-AP2	Windows Server 2008 R2 server running the DinnerNow .NET Application.
LON-MG1	Windows Server 2008 R2 server running an Operations Manager 2007 R2 Management Server.
LON-RMS	Windows Server 2008 R2 server running an Operations Manager 2007 R2 Root Management Server.
LON-SQ1	Windows Server 2012 R2 running SQL Server 2012 and Team Foundation Server 2012.
LON-SC1	Windows Server 2012 R2 running System Center 2012 R2 components.
LON-MS1	Windows Server 2012 R2 Server running a System Center 2012 R2 Management Server.
LON-MS2	Windows Server 2012 R2 Server running a System Center 2012 R2 Management Server.
LON-GW1	Windows Server 2012 R2 Server running a System Center 2012 R2 Gateway Server.
LON-SM1	Windows Server 2012 R2 running System Center 2012 R2 Service Manager.

Important If you are working in a local lab environment at the end of each lab, you may be instructed to revert the virtual machine to a previous checkpoint and not save any changes. Steps on how to do this are included at the end of each lab.

Software Configuration

The following software is installed on each VM:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008 R2

- SharePoint 2013 Server
- Team Foundation Server 2012
- SQL Server 2012
- SQL Server 2008 R2
- DinnerNow .Net Application
- System Center 2012 R2
- Operations Manager 2007 R2
- Visual Studio Professional 2010

Visio Professional 2013 Course Files

The files associated with the labs in this course are located in the <install_folder>\Labfiles\Lab10964B folder on the student computers.

Classroom Setup

Each classroom computer will have the same virtual machine configured in the same way.

You may be accessing the lab virtual machines in either in a hosted online environment with a web browser or by using Hyper-V on a local machine. The labs and virtual machines are the same in both scenarios however there may be some slight variations because of hosting requirements. Any discrepancies will be called out in the Lab Notes on the hosted lab platform.

You Microsoft Certified Trainer will provide details about your specific lab environment.

Course Hardware Level

Where labs are being run locally, to ensure a satisfactory student experience, Microsoft Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft Certified Partner for Learning Solutions (CPLS) classrooms in which Official Microsoft Learning Product courseware is taught.

Hardware Level 7 (Please note the change to the drive configuration for this course)

- 64 bit Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) processor (2.8 Ghz dual core or better recommended)
- Note: The two host machines provided for the instructor and each student must use the same processor architecture. Both host machines must be running either Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) processor, you cannot use one host machine with each processor architecture.
- Two 500 GB hard disks 7200 RPM SATA or faster. Each must be configured as a separate drive labeled Drive C and Drive D.
- 16 GB RAM or higher
- DVD drive
- Network adapter
- Dual SVGA monitors 17" or larger supporting 1440X900 minimum resolution
- Microsoft Mouse or compatible pointing device
- Sound card with amplified speakers

Module 1

Overview and Architecture

Contents:

Module Overview	1-1
Lesson 1: Overview of Operations Manager	1-2
Lesson 2: Overview of Key Features in Operations Manager	1-7
Lesson 3: Overview of Core Components and Topology	1-11
Lesson 4: Addressing Cloud and Datacenter Issues by Using Operations Manager	1-16
Lesson 5: Planning and Sizing System Center 2012 R2 Operations Manager	1-19
Lab: Using the System Center 2012 Operations Manager Sizing Helper Tool	1-27
Module Review and Takeaways	1-33

Module Overview

Before implementing Microsoft System Center 2012 R2 Operations Manager, it is important to understand the key features and functionality that it provides. This will help you understand how Operations Manager can be used to solve many common problems that arise in the cloud or datacenter, such as ensuring service levels are maintained and that critical line-of-business applications are available and performing at optimum levels.

Operations Manager is a comprehensive monitoring solution that requires careful planning before it is deployed into any IT environment. You must understand the hardware and software requirements of the solution and any security implications, such as those associated with monitoring computers in a trust boundary, perimeter network, or public cloud. When you configure the storage for the Operations Manager databases, you should have a good understanding of the number of computers and devices that are monitored to appropriately size the databases.

This module introduces students to the components contained in an Operations Manager Management Group and describes the dependency and relationships between the various components. Students will be shown how to plan for and design an Operations Manager Management Group.

Objectives

After completing this module, students will be able to:

- Describe the purpose and functionality of System Center 2012 R2 Operations Manager.
- Describe the key features of System Center 2012 R2 Operations Manager.
- Describe the System Center 2012 R2 Operations Manager components and topology.
- Describe the key cloud and datacenter problems that Operations Manager addresses.
- Describe how to design and size an Operations Manager Management Group.

Lesson 1

Overview of Operations Manager

System Center 2012 R2 has many components of which Operations Manager is only one. This lesson provides an overview of Microsoft System Center and the role that Operations Manager performs within the solution.

The key business drivers in choosing Operations Manager include why organizations use it to monitor and maintain their datacenters, and private and public cloud environments. This lesson also describes the key features and functions provided by Operations Manager and how Operations Manager integrates with other System Center components.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe, at a high-level, the components of System Center 2012 R2.
- Describe, at a high-level, the role of Operations Manager.
- Describe, at a high-level, the business drivers for choosing Operations Manager.

System Center 2012 R2 Components

System Center 2012 R2 helps you manage physical and virtual IT environments across private and public clouds, datacenters, client computers, and mobile devices. The following table provides a brief description of each System Center 2012 R2 component.

System Center 2012 R2 includes the following components:

- App Controller
- Configuration Manager
 - Endpoint Protection
- Data Protection Manager
- Operations Manager
- Orchestrator
- Service Manager
- Virtual Machine Manager
- System Center Advisor

System Center 2012 R2 component	Description
System Center 2012 R2 App Controller	Use the App Controller to manage, configure, and deploy services and virtual machines across public and private clouds.
Microsoft System Center 2012 R2 Configuration Manager	Configuration Manager provides features such as device management, operating system deployment, application deployments, and software update management for the Microsoft platform. Additionally, Configuration Manager provides configuration management that can detect and correct computers that are not compliant with the organization's compliance policies.
System Center 2012 R2 Endpoint Protection	Endpoint Protection provides desktop and server security management for the IT environment. Endpoint Protection is built on System Center 2012 R2 Configuration Manager and provides the same antimalware solution as Microsoft Security Essentials.
System Center 2012	Data Protection Manager (DPM) provides disk, tape, and cloud-based data

System Center 2012 R2 component	Description
R2 Data Protection Manager	protection and recovery for the Windows Server and Client operating systems. Protection for SQL Server, Exchange Server, Microsoft SharePoint Server, and Hyper-V is also supported. DPM can also centrally manage system state backups and bare-metal recovery (BMR).
System Center 2012 R2 Operations Manager	Operations Manager provides performance, health, and availability monitoring of the infrastructure, applications, and services in the IT environment.
System Center 2012 R2 Orchestrator	Orchestrator is an IT process automation solution that is used to automate the provisioning of resources and business processes in the IT environment.
System Center 2012 R2 Service Manager	Service Manager provides a platform to manage and automate the IT business processes. Additionally, Service Manager provides best practice methods for service management based on Microsoft Operations Framework and Information Technology Infrastructure Library.
System Center 2012 R2 Virtual Machine Manager	Virtual Machine Manager provides a virtualization management solution that is used to quickly create, manage, and deploy virtual machines and services to the private cloud.
System Center Advisor	System Center Advisor is an online service that utilizes Microsoft Azure to analyze the configuration of Microsoft Windows Servers and Applications.

More information about System Center 2012 R2 can be found at the following webpage:

System Center 2012 R2

<http://go.microsoft.com/fwlink/?LinkId=391262>

It should also be mentioned that although not strictly a component of System Center 2012 R2, the Windows Azure Pack which provides the ability to create self-service, multi-tenant clouds is also available as a no cost solution for Microsoft customers. Windows Azure Pack is built on top of Windows Server 2012 R2 and System Center 2012 R2. For more information about Windows Azure Pack visit the following website.

Windows Azure Pack for Windows Server

<http://go.microsoft.com/fwlink/?LinkId=404079>

Advantages of Using System Center 2012 R2 Operations Manager

To operate effectively, most organizations rely on IT as a core function. However, if the organization has no monitoring solution, the organization must rely on manual processes. These processes can include examining application logs or viewing performance graphs on servers to help resolve an issue or prevent a potential issue in the environment.

Operations Manager focuses on providing performance and availability information for all the IT infrastructure and applications. This includes hardware, software, and networking infrastructure.

Enterprise-ready monitoring solution for:

- Operating systems (server and desktop)
- Hardware
- Software
- Networking



Management Packs provide best-practice monitoring and a knowledge base



Built-in notifications, recoveries and diagnostics, and reporting and dashboards



Support for:

- Windows
- Linux
- UNIX



Note: Operations Manager also integrates with System Center Advisor and enables configuration assessment information and alerts generated by Advisor to be viewed in the Operations Manager Console.

Operations Manager includes proactive monitoring out of the box, and provides an early indication of a potential degradation in the performance of a service or a possible service outage. This lets you resolve the issue before it affects the business. To achieve this, Operations Manager uses Management Packs to provide best-practice monitoring and alerting that is targeted at a specific application or infrastructure component.

Typically, a Management Pack contains the following critical information: a set of discoveries that locate key application or infrastructure components, and several rules and monitors that have preconfigured thresholds based on the knowledge from developers and support engineers. So although the monitoring thresholds can be customized for any IT environment, they are (in many cases) set correctly out of the box according to best practice. Thus, monitoring can be up and running in the environment by using a minimum amount of effort.

In addition to providing an alerting mechanism that uses different channels such as email and Short Message Service (SMS), Operations Manager also includes automatic remediation of IT issues through diagnostic and recovery tasks. This can also be easily extended through the integration with the Orchestrator component of System Center 2012 R2 Orchestrator component. With this component, you can interoperate seamlessly with other management platforms, applications, and infrastructure components.

Rich reporting and dashboarding features are also included in Operations Manager. These features include the detailed analysis of the health, performance, and availability of the infrastructure and application components, and the awareness of the key SLA metrics. These reports and dashboards can be viewed by the operator through a console, emailed to a user, or directly published to a SharePoint portal so that they are consumed by the business.

IT environments differ greatly between organizations and can include a mixture of different operating systems such as Windows, Linux and UNIX, and many network devices. Operations Manager provides support for these different platforms without having to use a separate monitoring solution (or console) for each.

One of the new features in System Center 2012 R2 Operations Manager is Fabric Monitoring. By integrating System Center 2012 R2 VMM and System Center 2012 R2 Operations Manager, the

monitoring of both physical and virtual layers for private clouds is provided. Fabric Monitoring is covered in detail later in this course.

More information about Operations Manager can be found on the following webpage:



Getting Started with System Center 2012 - Operations Manager

<http://go.microsoft.com/fwlink/?LinkID=391263>

System Center 2012 R2 Operations Manager Business Drivers

When you select an enterprise monitoring solution such as System Center 2012 R2 Operations Manager, you might have to consider many business drivers before you decide on the most appropriate solution for the organization. For example, one main business driver might be to reduce the time-to-resolution of business-critical issues when they occur in the environment. When you reduce the time required to resolve an issue, your business services and applications are more likely to remain highly available, and thus you provide a more productive IT environment.

Business drivers to help choose the most appropriate monitoring solution include:

- Reduced time-to-resolution of business-critical issues
- Improved health of business services
- Unified management
- Dynamic and adaptive monitoring

Technically, several requirements might need to be satisfied to meet this business driver. For example, the solution would have to do the following:

- Include an alerting mechanism that is used for notifications that are sent through email and SMS when a business-critical issue is detected in the environment
- Store and retrieve resolution information by operators when troubleshooting a common issue
- Automatically correct issues when they occur
- Detect an issue before it adversely affects the business

Some other business drivers that can affect the decision regarding the most appropriate monitoring solution include those outlined in the following table.

Business driver	Technical requirements
Service Management	Provide visibility into the health and performance of business services by using reports and dashboards. The solution must be able to show whether SLAs are being met or not. Additionally, to ensure overall health, the solution should discover and represent all components of a business service in a single at-a-glance view
Systems Management	Reduce the overhead in managing different systems and platforms. The solution must provide a single console that is used to manage Windows, UNIX-based platforms, and Linux-based platforms. Networking infrastructure monitoring must also be included.
Application Health Management	Provide out-of-the-box performance and availability monitoring for commonly used applications. The solution should automatically apply default monitoring for common applications where monitoring thresholds are based on best-practice. It should also allow for customizations to default

Business driver	Technical requirements
	monitors and include automatic performance monitoring using baselines.
Dynamic and adaptive monitoring	Adapt to changes that occur in the IT environment without affecting business services. As new systems or devices are added to the IT environment, the solution must be able to automatically apply the most appropriate monitoring.

When you understand the business drivers, you can map the drivers to the features in the monitoring solution. This helps drive the business and provides a more proactive approach in how to manage and maintain the IT environment.

Question: How does Operations Manager provide best practice, out-of-the-box monitoring for your applications, computer systems, and devices?

Lesson 2

Overview of Key Features in Operations Manager

This lesson introduces the key features provided by Operations Manager and describes how to plan their implementation in your environment. You use this planning process to map business requirements to Operations Manager features and design your Management Group accordingly.

The lesson covers existing features in addition to new features introduced in Operations Manager 2012 R2.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe the key features in System Center 2012 Operations Manager.
- Describe the new features introduced with System Center 2012 R2 Operations Manager.

Key Features in System Center 2012 Operations Manager

If you are familiar with Operations Manager 2007 R2, you know about some of the important features available in System Center 2012 Operations Manager. However, many of these existing features have been extensively upgraded since Operations Manager 2007 R2. The following table describes some of the upgraded features, which are available in System Center 2012 Operations Manager. Features in both System Center 2012 Operations Manager and System Center 2012 Service Pack 1 (SP1) Operations Manager are included in the following table.

Key features in System Center 2012 Operations Manager include:

- Application performance monitoring (APM)
- Network monitoring
- Dashboards
- Web console
- UNIX-based and Linux-based monitoring
- Transaction monitoring
- Management Pack templates
- Team Foundation Server (TFS) integration

System Center 2012 Operations Manager feature	Description
APM	In addition to the extensive Management Packs that are available to monitor Microsoft and non-Microsoft applications, Operations Manager includes built-in support for monitoring applications developed with the .NET Framework and Java Enterprise Edition (Java EE) platform. The APM feature provides performance and availability monitoring from both the server-side and client-side perspective. Two new Web consoles are included that provide root cause analysis and reporting on exception events detected in applications based on .NET and Java EE. APM is covered in detail Module 5, "Application Performance Monitoring."
Network monitoring	Network monitoring has been significantly improved in System Center 2012 Operations Manager. With support for over 80 network device manufacturers, monitoring for almost all network devices is possible, including port monitoring. For devices that support it, extended monitoring capabilities such as memory and CPU use can also be enabled.
Dashboards	Visualizing data collected by Operations Manager is critical to understanding how an application or service is performing. Dashboards provide a method of displaying the health and

System Center 2012 Operations Manager feature	Description
	availability of any object monitored by Operations Manager in a single view. This removes the need to browse through multiple views to obtain performance metrics, alerts, and health state, because all of this can be included in a single dashboard. Summary, SLA, and Network dashboards are included out of the box, and you can easily create new dashboards that combine data such as performance metrics, alerts, SLA metrics, and health state. After they are created, dashboards can be viewed in either the Operations console or Web console, and they can also be published to a SharePoint webpage by using the Operations Manager SharePoint Web Part. This means that people who do not have access to the Operations console or Web console can still view performance, health, and availability metrics for applications and services monitored by Operations Manager.
Web console	With the release of System Center 2012 SP1, the Operations Manager Web console has been updated to improve load time and uses Microsoft Silverlight. Thus, IT pro dashboards can be displayed in the Web console.
UNIX-based and Linux-based monitoring	<ul style="list-style-type: none"> • In System Center 2012 SP1 Operations Manager, UNIX and Linux monitoring has been improved and now includes: • CentOS 5 (x86/x64) • CentOS 6 (x86/x64) • Debian GNU/Linux 5 (x86/x64) • Debian GNU/Linux 6 (x86/x64) • Oracle Linux 5 (x86/x64) • Oracle Linux 6 (x86/x64) • Ubuntu Server 10.04 (x86/x64) • Ubuntu Server 12.04 (x86/x64)
Transaction monitoring	With the release of System Center 2012 SP1, additional transaction monitoring capabilities are included, which extend Operations Managers ASP.NET web application and ASP.NET web service monitoring. Transaction monitoring for the Windows service and Windows Communication Foundation (WCF) service is also included.
Management Pack templates	Management Pack templates provide a quick and simple wizard-driven method of extending the monitoring that Operations Manager provides. In addition to the standard Management Pack templates such as OLE DB Data Source, TCP Port, Windows Service, and Process Monitor, templates for monitoring .NET applications, web application availability, and web application transaction monitoring are now included.
Team Foundation Server (TFS) integration	With the release of System Center 2012 SP1 Operations Manager, integration with Team Foundation Server 2010 and 2012 is provided. This gives you the ability to synchronize Operations Manager alerts with work items in TFS.

The list of features in the preceding table is by no means exhaustive and is provided to show only some of the key features that are included with System Center 2012 Operations Manager and System Center 2012 SP1 Operations Manager. These features, including standard features such as reporting, Audit Collection Services (ACS), and Agentless Exception Monitoring (AEM), are covered in detail later in this course.

New Features in System Center 2012 R2 Operations Manager

Additional features and enhancements were included in the release of System Center 2012 R2 Operations Manager. The following table below describes these features.

New features in System Center 2012 R2 Operations Manager include:

- Fabric Monitoring
- Microsoft Monitoring Agent
- TFS integration enhancements
- IP 6 support
- Java Application Performance Monitoring
- System Center Advisor integration
- UNIX and Linux monitoring

System Center 2012 R2 Operations Manager feature	Description
Fabric Monitoring	As mentioned in the module overview of System Center 2012 R2 Operations Manager, the new Fabric Monitoring feature provides support for monitoring both physical and virtual layers for hybrid private clouds. After integration between VMM and Operations Manager is configured, a new dashboard, the Fabric Health Dashboard, is available in the Operations console. This dashboard can be used to view the health state of clouds and associated resources in VMM.
Microsoft Monitoring Agent	The Operations Manager agent has been replaced in System Center 2012 R2 Operations Manager with the Microsoft Monitoring Agent. This agent combines the monitoring provided by .NET APM and Microsoft Visual Studio IntelliTrace Collector. This allows for full application profiling traces to be collected for .NET applications and then saved in the IntelliTrace format, at which point they can be opened in Visual Studio Ultimate.
TFS integration enhancements	Two new alert fields are now available: TFS Work Item ID and TFS Work Item Owner. These read-only fields provide details about which work items in TFS are related to specific alerts in Operations Manager and who the work items are assigned to. In addition, performance events collected by APM can now be converted to IntelliTrace format and then assigned to work items in TFS.
IPv6 support	When configuring network device monitoring in Operations Manager, IPv6 notation can now be used when configuring network discovery rules. IPv6 notation is also supported in the network monitoring-related views in the Operations console.
Java Application Performance Monitoring	A new Management Pack named System Center 2012 Management Pack for Java Application Performance Monitoring provides performance and exception event monitoring for Java-based applications.
System Center Advisor integration	System Center Advisor is a Microsoft online service that analyzes configurations of Microsoft servers and provides alerting when servers are found not to be configured according to best practice. With System Center 2012 Operations Manager SP1 update rollup 2 and newer versions, you can now view System Center Advisor alerts in the Operations Console.
UNIX and Linux monitoring	UNIX and Linux monitoring have been extended in System Center 2012 R2 Operations Manager to include support for Debian GNU/Linux 7.

For more information on the new features in System Center 2012 R2 Operations Manager visit the following website.

 **What's New in System Center 2012 R2 Operations Manager**

<http://go.microsoft.com/fwlink/?LinkId=404080>

Question: What function does the new Fabric Monitoring feature in System Center 2012 R2 Operations Manager provide?

Lesson 3

Overview of Core Components and Topology

To design and implement a new Operations Manager environment, you must have an understanding of the core components contained in a Management Group. With this knowledge, you will be able to design a solution that meets your business, technical, and security needs, including planning for monitoring components in untrusted domains or perimeter networks.

This lesson describes Operations Manager topology and core components in addition to various different design scenarios, including designing for high availability.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe the core components of Operations Manager.
- Describe the topology of Operations Manager.
- Describe high availability options in Operations Manager.

Operations Manager Core Components

When Operations Manager is deployed, the core components are known as a *Management Group*. When you deploy Operations Manager, you are prompted to provide a Management Group name. This is used to differentiate Management Groups in a multi-Management Group scenario, such as in a multitenant environment.

Several key components are included in Operations Manager. Each component is described in the following table.

Operations Manager core components include:

Core Components	Core Components
Management Server	Operations console
Databases	Web console
Agents	Application Advisor and Application Diagnostic consoles
Reporting	
Management Packs	Gateway Server

Operations Manager component	Function
Management Server	Management Servers primarily provide a communication channel between the Operations Manager database server and the managed computers in the Management Group.
Databases	Operations Manager has two main databases, an Operational database (OperationsManager) and a data warehouse database (OperationsManagerDW). These databases store discovery, event, alert, and performance data. They also include configuration data about the Management Group.
Agents	Agents are installed on computers that must be monitored by Operations Manager and can include Windows, UNIX-based, and Linux-based systems. Agentless monitoring is also possible on systems where an agent cannot be deployed, such as on secure systems with restricted access.
Reporting	Reporting uses SQL Server Reporting Services (SSRS). You can use this to visualize data that is contained in the data warehouse.

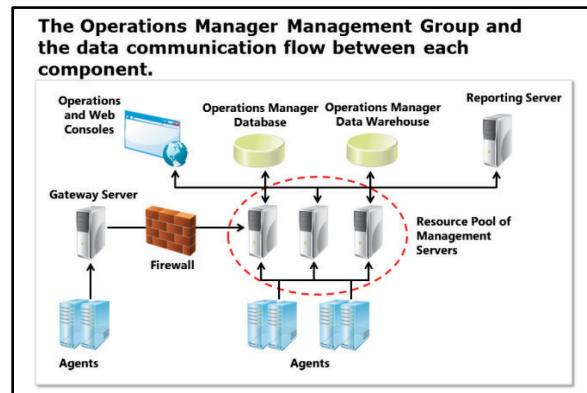
Operations Manager component	Function
	database and reports are then typically accessed from the Operations console.
Management Packs	Management Packs are the basic unit of instruction in Operations Manager. Management Packs are targeted at certain types of application, platform, or infrastructure, and contain all the important information that is required to enable monitoring. A Management Pack can include (but is not limited to) Rules, Monitors, Scripts, Discovery Mechanisms, Overrides, Tasks, Dashboards, and Reports. Typically, a Management Pack contains knowledge base information that explains the issues that have occurred and the resolution paths or fixes.
Operations console/Web console	Both the Operations console and the Web console provide a view of monitoring based on the Management Packs that you have deployed. Additionally, the Operations console is used to access administration, authoring, and reporting functions.
Application Advisor and Application Diagnostics consoles	These consoles are used together with the Application Performance Monitoring (APM) feature of Operations Manager. They provide diagnostic details and reports on the Microsoft .NET Framework and Java-based applications and services that are being monitored.
Gateway Server	In an environment where there is no Kerberos authentication between an agent and a Management Server (such as in a non-trusted domain or perimeter network), mutual authentication is enabled by the implementation of a secure certificate from a trusted certification authority (CA). If there are several agents in this scenario (typically five or more), we recommend that you implement an Operations Manager Gateway Server. This reduces the administration overhead. The certificate is then implemented between the Gateway Server and the Management Server. Then, the agents communicate with the Management Server through the Gateway Server. This removes the need for the certificate to be installed on each agent. Gateway Servers are also used when the network traffic from many agents located in a remote site must be reduced. Gateway Servers are also used for a local administration function in a remote site such as deploying agents. In scenarios where workgroup computers are to be monitored, certificates must be used to provide mutual authentication between the agent-managed computer and its associated Management Server. Note that Gateway Servers can also be utilized in remote locations or sites where network latency is high between the local site (where the Operations Manager operational database resides) and the remote site (where agent-managed computers reside). As the Gateway server connects directly to a Management Server, it does not require a low-latency connection to the Operations Manager operational database. In addition all Management Servers in an Operations Manager Management Group should be able to communicate over a low-latency network. So in locations where there is high network latency you should consider using a Gateway Server instead of a Management Server for agent-managed computers.

Operations Manager Topology

The following sections describe how communication works between components in a Management Group.

OperationsManager and OperationsManagerDW Databases

The Operations Manager databases contain all information that relate to the Management Group. This includes the monitoring data that is collected by agents that run on managed computers and the configuration of the Management Group that includes the Management Packs that are deployed in the environment. The direct communication between the Management Servers and the Operations Manager databases is described in the sections that follow.



 **Note:** SQL Server AlwaysOn is also supported in Operations Manager and is covered in detail in *Module 11: Troubleshooting, Tuning, and Disaster Recovery*.

Management Servers

Management Servers insert monitored data into the Operations Manager databases that are forwarded from the Operations Manager agent that runs on the managed computers. Additionally, Management Servers communicate with other Management Servers to provide load balancing and failover. This is discussed in more detail in the next topic.

Gateway Servers

The Gateway Server sends collected monitoring data (forwarded by agents that report to it) to its associated Management Server for insertion into the Operations Manager databases. By default, this connection is initiated by the Gateway Server. However, you can change the direction of this communication when the gateway installation is approved.

Agents

Agents communicate with the Management Servers (or Gateway Servers) that they are assigned to. The agents forward any relevant monitoring data back to the Management Server for insertion into the Operations Manager databases. This connection is initiated by an agent, although communication is bidirectional.

Consoles

The Operations console connects to the Management Server so that the operators can manage and administer Operations Manager functions. Similarly, the Web console server communicates with the Management Server to display monitoring data in the Web console. Additionally, the Web console for Application Diagnostics uses the OperationsManager database to display event details that are collected for application performance monitoring. The Web console for Application Advisor uses the OperationsManagerDW database to collect data for application performance monitoring reports.

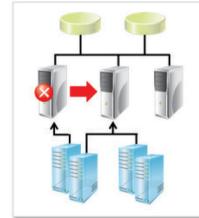
Reporting Servers

The Reporting Server is deployed on a SSRS instance that retrieves data from the Operations Manager data warehouse database. Access to reports is provided from the Reporting pane in the Operations console.

High Availability in Operations Manager

Since Operations Manager 2012, the root management server (RMS) concept has been deprecated. By adding multiple Management Servers, the workflows previously run only on the earlier RMS component are now automatically applied across all Management Servers in the Management Server resource pool. If a Management Server stops, the workflows that run on that server are automatically retrieved by the remaining Management Servers in the pool. This new concept removes the need to cluster the RMS component for high availability.

- High Availability is included
- All Management Servers are considered equal
- When a Management Server fails, the workload is moved to another Management Server in the resource pool



New in Operations Manager 2012 is better reliability for consoles through the availability of the software development kit (SDK) service on all Management Servers. (In Operations Manager 2007, console access is provided only through the SDK service that runs on the RMS). Automated failover for consoles can now also be provided through the implementation of Network Load Balancing (NLB) for console connections.

To enable backward compatibility for connectors or earlier Management Packs that are written to target the earlier RMS role, an RMS Emulator role exists in Operations Manager 2012. This role is static and resides on the first Management Server that you install or on the server where the earlier RMS role existed in the Operations Manager 2007 upgrade scenario. The RMS emulator role can be moved to a different Management Server by using a Windows PowerShell command.

Operations Manager Resource Pools

The resource pool is a new feature in Operations Manager. The resource pool hosts a collection of Management Servers that work together to provide load balancing and high availability for workloads that run in a Management Group. If one of the Management Servers becomes unavailable, the other Management Servers in the pool automatically retrieve the workloads that they are running.

By default, after you install Operations Manager, three resource pools are created to run RMS-specific workloads. These workloads include those described in the following sections.

All Management Servers Resource Pool

This pool is used to target the most common RMS-type workloads, such as Group Calculation, Availability, Distributed Health Roll-Up, and DB Grooming. All Management Servers automatically become a member of this pool.

Notifications Resource Pools

This pool is used to target Alert Subscription Service workloads. By using a separate pool (other than the All Management Servers resource pool), you can make sure that only the necessary Management Servers host the Alert Subscription workloads. For example, you might have five Management Servers, but only two of the Management Servers have an SMS modem attached. In this scenario, the three Management Servers that do not have an SMS modem attached can be removed from the pool.

AD Assignment Resource Pool

This pool is used to target Active Directory assignment workflows that manage the agent to the Management Server association, when Active Directory integration is configured. Again, by segregating these workloads into a separate pool, you can control the Management Servers that should be used for this role.

In addition to the default resource pools discussed, you can create new resource pools in Operations Manager. For example, when you monitor network devices, or UNIX-based and Linux-based computers, you can also create a resource pool to provide high availability for these workloads.

Resource pools can also be used with Web Application Availability Monitoring in Operations Manager. When you use the Add Monitoring Wizard to configure the monitor, instead of selecting specific computers (agents) on which the monitoring should be initiated, you can select a resource pool. This provides high availability for workloads that are related to Web Applications Availability Monitoring.

Management Servers in a resource pool must communicate with one another in a timely manner to determine the Management Servers that are available to handle workloads at any time. Therefore, it is recommended that all Management Servers be connected over a low latency network. If you currently use Management Servers in different datacenters or sites, you should move all Management Servers to a central site and use Gateway Servers in those locations instead.

A recommended best practice is to always have a minimum of two Management Servers in your environment to allow for failover or restore.

The SDK Service is now available and running on every Management Server, and changes were made to the Configuration Service in Operations Manager. In Operations Manager 2007, when the Configuration Service started on a Management Server, it loaded its required view of configuration into memory in XML. However, this is not practical in Operations Manager, because this service is distributed across all members of a resource pool. Now, this data is stored in the operational database and it is queried when it is necessary. This results in a much faster startup of Management Servers. Because of this new feature, it is also recommended that communication between the Management Server and the operational database occur over a low latency network.

Question: What is the primary function of a Gateway Server in Operations Manager?

Lesson 4

Addressing Cloud and Datacenter Issues by Using Operations Manager

It is important that you understand the issues that Operations Manager addresses both in the cloud and in the datacenter. This will help you design your Operations Manager Management Group appropriately so that it provides effective monitoring for your applications, services, infrastructure, and cloud resources, such as networking, storage, and compute.

For example, one of the key problems that cloud and datacenter administrators face is knowing whether business critical services and applications are available and performing within their service level agreements (SLAs). In most organizations, a failing business-critical application at best could result in a degradation in service. At worst, it could mean a disruption of service and potential loss of both revenue and customer satisfaction.

In this lesson, you will learn about some of the important issues that Operations Manager addresses in both the cloud and datacenter environments.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe key problems that Operations Manager addresses in the cloud.
- Describe key problems that Operations Manager addresses in the datacenter.

Operations Manager in the Cloud

When administering a private cloud, it is important that the underlying resources (or fabric) on which both the cloud and associated applications and services rely be available at all times. This fabric includes resources such as networking, storage, and compute. It is equally important that the virtualization technology managing your private clouds also be available and performing at optimum levels. Without an appropriate monitoring solution in place, manual tasks must be performed to ensure these resources are always online. These tasks could include reviewing event logs, and checking performance counters and available disk space. Monitoring the private cloud environment manually is a time-consuming task and can often lead to problems going undetected until an end user reports a problem with accessing a service or application. System Center 2012 R2 addresses this problem by integrating Operations Manager and Virtual Machine Manager (VMM) and implementing the System Center Management Pack for VMM Fabric Dashboard 2012 R2. By integrating Operations Manager and VMM, you extend Operations Manager monitoring capabilities to the private cloud. Integrating Operations Manager and VMM is covered in greater detail later Module 4, "Configuring Fabric and Application Monitoring."

When you move applications and services to a public cloud such as Microsoft Azure, it is important that these applications and services are available and performing at acceptable levels. Although you do not have control of the underlying fabric that the public cloud relies upon, it is critical that the network, storage, and compute resources are monitored to ensure your applications and services remain available.

Operations Manager can monitor private clouds by:

- Integrating Operations Manager and VMM
- Implementing the System Center Management Pack for VMM Fabric Dashboard 2012 R2



Operations Manager can monitor public clouds by:

- Implementing the System Center Management Pack for Windows Azure Fabric
- Implementing the System Center Monitoring Pack for Windows Azure Applications Management Pack



Until now, monitoring resources in the public cloud was not possible. This meant that you had to rely on reports from your service provider to confirm that your applications and services were available and service level goals were met. With System Center 2012 R2 Operations Manager, this issue is addressed by the System Center Management Pack for Windows Azure Fabric. After installing and configuring the Management Pack, Operations Manager monitoring is extended to the Microsoft Azure public cloud. Fabric resources such as cloud services, storage, and virtual machines can now be monitored in Operations Manager. An additional Management Pack named System Center Monitoring Pack for Windows Azure Applications is also available to extend the ability of Operations Manager to monitor the health and availability of applications running on Microsoft Azure. The System Center Management Pack for Windows Azure Fabric and the System Center Monitoring Pack for Windows Azure Applications Management Packs are covered in greater detail in Module 4.

Operations Manager in the Datacenter

IT in the datacenter includes a number of components such as networking, servers, workstations, applications, and services. Monitoring effectively without an appropriate monitoring solution is very difficult. The datacenter administrator must ensure that all IT services are available at all times for the business to function, so proactive monitoring of key systems is essential.

For example, you might have a line-of-business application that users in your organization require on a daily basis to perform their jobs. If this application becomes unavailable, those users will not be able to perform their jobs satisfactorily. To monitor the application effectively, you should include in your monitoring scope the application and any underlying components that it relies upon, such as Windows Server, Microsoft Internet Information Services (IIS), and Microsoft SQL Server. You should also include any networking infrastructure that the application replies upon when it communicates with other components. Without a monitoring solution such as System Center 2012 R2 Operations Manager, you would have to manually check each component's health and availability to ensure the application is running at all times. Performing these tasks would not only take an enormous amount of time, but also could lead to application failures resulting from potential issues not being detected in time.

Another element of the application that should be monitored is the end-user experience. If your organization uses applications from multiple locations, you need to ensure that users at each location can access the application. This would be a very difficult task for the datacenter administrator to perform manually, because the administrator would need to visit each location and test the application locally.

By using System Center 2012 R2 Operations Manager, you take advantage of distributed application diagrams and synthetic transactions to address these challenges. A *distributed application diagram* provides a single view that contains all monitored components of an application or service. The view is updated to show the health and availability of each component that the application relies on, so you can instantly become aware of any detected problems. You can use *synthetic transactions* to simulate the end users' access to the application from any location where an Operations Manager agent is installed. Thus, you can both determine how an application is performing from an end users' perspective and obtain useful troubleshooting information when an application is performing poorly. These synthetic transactions can also be included in distributed application diagrams to complete the full-spectrum monitoring that

Operations Manager provides proactive monitoring in the data center and includes:

Distributed Application Diagrams

Provides a single view to show the health and availability of all components that constitute an application or service



Synthetic transactions

Monitors applications and services from the user's location to give a representation of the user's experience when using applications or services

Operations Manager provides. Synthetic transactions and distributed application diagrams are covered in greater detail later in this course.

By using Operations Manager to monitor your datacenter, you provide proactive monitoring that ensures your business-critical applications and services are available at all times.

Question: You need to create a single view that can be used to monitor all components of a line-of-business application. What feature of Operations Manager can help you achieve this?

Lesson 5

Planning and Sizing System Center 2012 R2 Operations Manager

Before deploying a new Operations Manager 2012 R2 Management Group in your environment, you should consider many factors, such as hardware and software requirements. The solution must be designed to scale to the planned number of computers and network devices that will be managed, because this will have a direct relationship on the size of the Operations Manager databases and number of Management Servers.

The features enabled in the Management Group such as Agentless Exception Monitoring (AEM), Audit Collection Services (ACS), and Application Performance Monitoring (APM) will also impact the size and design of the solution.

You should consider the topology of your IT environment, including any trust boundaries or perimeter networks that contain computers or devices that you intend to monitor, and consider whether the environment needs to be extended into a public cloud infrastructure. You might also need to factor in the addition of a Gateway Server to assist with monitoring these components, or you might need to set up certificates for a Microsoft Azure subscription.

Lesson Objectives

- Describe the hardware and software requirements of System Center 2012 R2 Operations Manager.
- Describe the firewall considerations with System Center 2012 R2 Operations Manager.
- Describe how to use the System Center 2012 Operations Manager Sizing Helper tool to help plan for an Operations Manager deployment.

System Center 2012 R2 Operations Manager Hardware and Software Requirements

Before you can deploy Operations Manager, you must understand the hardware and software requirements of each component. This is important because you might have to obtain additional hardware or software, or you might have to provide additional hardware for high-quality availability. If you plan to use virtual machines to host some or all of the Operations Manager components, you should be aware that although Microsoft supports running any Operations Manager component in a virtual environment, it is recommended that the

OperationsManager and OperationsManagerDW databases be stored on a directly-attached physical hard disk drive. This helps make sure that data can be written and read from the Operations Manager databases in a timely manner to improve the overall Management Group performance.

Whether you plan to deploy Operations Manager to a physical or virtual environment, you must carefully consider several factors, including how many computers and network devices in the environment will be monitored. This number greatly affects the sizing of the Operations Manager databases. Additionally, you should consider your data retention requirements. By default, data is retained in the OperationsManager database for 7 days, and in the OperationsManagerDW database for up to 400 days.

Hardware and software requirements for:

- Management Server
- Database Server
- Agents
- Gateway Server
- Reporting Server
- Operations Console
- Web Console

The following lists outline the minimum hardware and software requirements for each Operations Manager component.

Management Server Requirements

- **Disk space.** %SYSTEMDRIVE% requires at least 1024 megabytes (MB) of free hard disk space.
- **Server operating system.** Windows Server 2008 R2 Service Pack 1 (SP1), Windows Server 2012, Windows Server 2012 Core Installation, or Windows Server 2012 R2.
- **Processor architecture.** x64.
- **Memory.** A minimum of 2 gigabytes (GB) of memory is required but 4 GB is recommended.
- **Windows PowerShell version.** Windows PowerShell 2.0, Windows PowerShell 3.0, or Windows PowerShell 4.0.
- **Windows Remote Management.** Windows Remote Management enabled for the Management Server.
- **Windows Identity Foundation.** Required for the Management Server role for Advisor.
- **.NET Framework.** .NET Framework 4 or .NET Framework 4.5.

Operational Database and Data Warehouse Database Server Requirements

- **Disk space.** Operational database must have at least 1024 MB of free disk space.
- **File system.** %SYSTEMDRIVE% formatted with the NTFS file system.
- **Operating system.** Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation, or Windows Server 2012 R2.
- **Processor architecture.** x64.
- **Memory.** A minimum of 4 gigabytes (GB) of memory is required but 8 GB is recommended.
- **Windows installer version.** At least Windows Installer 3.1 is required.
- **SQL Server.** SQL Server SQL 2008 R2 Service Pack 1 (SP1), SQL Server 2008 R2 Service Pack 2 (SP2), SQL Server 2012, or SQL Server 2012 Service Pack 1 (SP1).
- **SQL Server full-text search.**
- **.NET Framework.** .NET Framework 4.

Agent Requirements (Windows-based Computers)

- **File system.** %SYSTEMDRIVE% formatted with the NTFS file system.
- **Operating systems.** One of the following: Windows Server 2003 Service Pack 2 (SP2), Windows Server 2008 Service Pack 2 (SP2), Windows Server 2008 R2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows XP Professional x64 Edition Service Pack 2 (SP2), Windows XP Professional Service Pack 3 (SP3), Windows Vista Service Pack 2 (SP2), Windows 7, POSReady, Windows XP Embedded Standard, Windows XP Embedded Enterprise, Windows XP Embedded POSReady, Windows 7 Professional for Embedded Systems, Windows 7 Ultimate for Embedded Systems, Windows 8 Pro, or Windows 8 Enterprise.
- **Processor architectures.** x64 or x86.
- **Memory.** Determined by Operating System requirements.
- **Microsoft Core XML Services (MSXML) version.** Microsoft Core XML Services 6.0 is required for the Operations Manager agent for Windows Server 2003.
- **Windows PowerShell version.** Windows PowerShell 2.0 or Windows PowerShell 3.0.

Agent Requirements (UNIX-based or Linux-based Computers)

- CentOS 5 and 6 (x86/x64)
- Debian GNU/Linux 5, 6, and 7 (x86/x64)
- HP-UX 11i 2 and 3 (PA-RISC and IA64)
- IBM AIX 5.3, AIX 6.1 (POWER), and AIX 7.1 (POWER)
- Novell SUSE Linux Enterprise Server 9 (x86), Enterprise Server 10 SP1 (x86/x64), or Enterprise Server 11 (x86/x64)
- Oracle Solaris 9 (SPARC), Solaris 10 (SPARC and x86), or Solaris 11 (SPARC and x86)
- Oracle Linux 5 and 6 (x86/x64)
- Red Hat Enterprise Linux 4, 5, and 6 (x86/x64)
- Ubuntu Linux Server 10.04 and 12.04 (x86/x64)
- **Memory.** Determined by Operating System requirements.

Report Server Requirements

- **Disk space.** %SYSTEMDRIVE% with at least 1024 MB of free hard disk space.
- **Operating system.** Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation, or Windows Server 2012 R2.
- **Processor architecture.** x64.
- **Memory.** A minimum of 1 gigabyte (GB) of memory is required but 2 GB is recommended.
- **SQL Server.** SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1.
- **Remote Registry Service.** Must be enabled and started.
- **SQL Server Reporting Services.** SQL Server SQL 2008 R2 SP1, or SQL Server 2008 R2 SP2, or SQL Server 2012, or SQL Server 2012 SP1.
- **System Center 2012 Operations Manager.** Supports SQL Server Reporting Services in native mode only; do not use SharePoint integrated mode.
- **.NET Framework.** .NET Framework 4.

Gateway Server Requirements

- **Disk space.** %SYSTEMDRIVE% requires at least 1024 MB of free hard disk space.
- **Server operating system.** Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 Core Installation, or Windows Server 2012 R2.
- **Processor architecture.** x64.
- **Memory.** A minimum of 2 gigabytes (GB) of memory is recommended.
- **Windows PowerShell version.** Windows PowerShell 2.0, or Windows PowerShell 3.0.
- **Microsoft Core XML Services (MSXML) version.** Microsoft Core XML Services 6.0 is required for the Management Server.
- **.NET Framework.** .NET Framework 4 is required if the Gateway Server manages UNIX/Linux agents or network devices.

Operations Console Requirements

- **Report Viewer.** Microsoft Report Viewer 2012 Redistributable Package
- **Disk space.** %SYSTEMDRIVE% requires at least 512 MB free hard disk space.
- **File system.** %SYSTEMDRIVE% must be formatted with the NTFS file system.
- **Server Operating System.** Windows 7, Windows 8, Windows Server 2008 R2 SP1, Windows Server 2012, or Windows Server 2012 R2.
- **Processor Architecture.** x64 for servers, and x64 or x86 for a client computer.
- **Memory.** A minimum of 2 gigabytes (GB) of memory is required but 4 GB is recommended.
- **Windows Installer version.** At a minimum, Windows Installer 3.1.
- **Windows PowerShell version.** Windows PowerShell 2.0. Windows PowerShell 3.0 is required to use Windows PowerShell cmdlets for administration of UNIX-based and Linux-based computers.
- **.NET Framework.** .NET Framework 4.

Web Console Server Requirements

- **Operating System.** Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2.
- **Processor Architecture.** x64.
- **Memory.** A minimum of 1 gigabyte (GB) of memory is required but 2 GB is recommended.
- **Web browsers.** Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, Internet Explorer 11, Silverlight 5.0.
- **IIS 7.5 and newer versions, with the IIS Management Console and the following role services installed:**
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - HTTP Logging
 - Request Monitor
 - Request Filtering
 - Static Content Compression
 - Web Server (IIS) Support
 - IIS 6 Metabase Compatibility
 - ASP.NET (both ASP.NET 2.0 and ASP.NET 4. are required)
 - Windows Authentication
- **Selected website for Web console.** Requires a configured http or https binding.
- **.NET Framework.** .NET Framework 4.

For more information about the hardware and software requirements for System Center 2012 R2 Operations Manager visit the following website.



System Requirements: System Center 2012 R2 Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=404081>

System Center 2012 R2 Operations Manager Firewall Requirements

Many Operations Manager components can be installed on separate computers and will provide flexibility and load balancing of the overall Management Group. If the components must communicate through a firewall, you must be aware of the firewall port exceptions that must be configured.

The following table shows each Operations Manager component. This includes the port that it uses to communicate with other Operations Manager components. The table also shows the direction in which the firewall exception should be configured.

You might need to create firewall exceptions when:

- A computer or device resides in a perimeter network
- You need to monitor computers within a trust boundary
- A firewall exists between two Operations Manager components that must communicate

Operations Manager component	Firewall port and direction	Operations Manager component
Management Server	1433 →	Operational database
Management Server	← 1434 UDP	Operational database
Management Server	5723, 5724 →	Management Server Note: Port 5724 is used to install the feature and can be closed after the feature is installed.
Management Server	1433 →	Reporting data warehouse
Reporting Server	5723, 5724 →	Management Server
Operations console	5724 →	Management Server
Connector Framework source	51905 →	Management Server
Web console server	Selected website port →	Management Server
Web console (for Application Diagnostics)	1433 →	Operational database
Web console (for Application Advisor)	1433 →	Data warehouse
Web browser	80, 443 →	Web console server
Agent installed by using MOMAgent.msi	5723 →	Management Server
Agent installed by using MOMAgent.msi	5723 →	Gateway Server
Gateway Server	5723 →	Management Server
Agent (ACS forwarder)	51909 →	Management Server ACS Collector

Operations Manager component	Firewall port and direction	Operations Manager component
Agentless Exception Monitoring data from client	51906 →	Management Server AEM file share
Customer Experience Improvement Program (CEIP) data from client	51907 →	Management Server (CEIP) endpoint
Operations console (reports)	80 →	SQL Server Reporting Services
Reporting Server	1433 →	Reporting data warehouse
Management Server (ACS Collector)	1433 →	ACS database
Management Server	← 161, 162 →	Network device (UDP or ICMP)
Management Server or Gateway Server	1270 →	UNIX-based or Linux-based computer
Management Server or Gateway Server	22 →	UNIX-based or Linux-based computer

The System Center 2012 Operations Manager Sizing Helper Tool

To help with planning an Operations Manager deployment, the System Center 2012 Operations Manager Sizing Helper tool 1.0 can be used to provide recommendations for hardware that will be required to deploy an Operations Manager Management Group based on factors such as the number of monitored computers and devices. The tool is divided into four main sections as described here.

Getting Started

In the Getting Started section, a Supported Configuration page provides the monitored items capacity of key Operations Manager components. This covers the number of supported agents per Management Server and the number of supported agents for application performance monitoring per Management Group. This section is useful in obtaining an overview and idea of the size of your Management Group. For example, if you have 4,000 Windows-based computers to manage, you can quickly determine that you will require a minimum of two Management Servers in your Management Group to support this. Also provided in this section are best-practice guidelines that should be followed when deploying an Operations Manager Management Group, including guidelines addressing disk configuration high availability, network monitoring, and virtualization.

Standard Deployment

In the Standard Deployment section, you can quickly obtain the minimum hardware recommendation for a standard Operations Manager Management Group that includes monitoring for Windows-based computers and network devices, and application performance monitoring. On this page, you configure

When using the System Center 2012 Operations Manager Sizing Helper tool, you specify:

- The number of Windows-based computers to monitor
- The number of network devices to monitor
- Whether APM should be enabled

The System Center 2012 Operations Manager Sizing Helper tool provides recommendations for:

- Number of Management Servers
- Hardware for Management Servers, operational database, and data warehouse database
- Hardware for Web console server and Reporting Services server

the number of Windows-based computers, the number of network devices, and whether APM is to be enabled. After configuring these values, you then click Submit. The minimum hardware recommendations are then calculated and displayed. Included in the minimum hardware recommendation is the number of Management Servers required; the number of Management Servers per resource pool; and the disk, CPU, and memory required for each Operations Manager role. Database sizes based on configurable data retention is also provided. This is useful because you can amend the data retention values for the operational and data warehouse databases and then recalculate the required database sizes. You can also amend other factors such as the number of monitored computers or network devices, and then recalculate the recommended hardware requirements.

Advanced Deployment

In the Advanced Deployment section, you can obtain the minimum hardware recommendation for Gateway Servers, UNIX or Linux monitoring, and URL monitoring. For both UNIX or Linux monitoring and URL monitoring, a formula is provided, which is useful when you need to calculate, for example, the number of agents supported in a Management Server pool.

Advanced Database Sizing

In the Advanced Database Sizing section, three additional calculators are provided to help determine the operational database size, the data warehouse database size, and the disk configuration recommended for each. These calculators are explained further in the following table.

Calculator	Description
DB Size Calculator	The DB Size Calculator calculates the operational database size based on configurable factors such as data retention, number of server computers, number of network devices, and the number of APM-enabled computers. After specifying these values, the total database size is calculated in megabytes and gigabytes. Also provided is the estimated number of I/O operations per second (IOPS) based on the number of agents monitored.
DW Size Calculator	The DB Size Calculator calculates the data warehouse database size. This calculator works in exactly the same manner as the DB Size Calculator.
DB DW Disk Calculator	The DB DW Disk Calculator provides a recommended disk configuration based on the estimated disk space obtained from the DB and DW Size Calculators, and on the estimated IOPS from the DB and DW Size Calculators. After specifying these values, the estimated number of RAID disks required is calculated. This is based on a RAID 10 and RAID 5 configuration.

When you have determined the number of monitored computers, network devices, data retention requirements, and application performance monitoring requirements, the System Center 2012 Operations Manager Sizing Helper tool should be used to obtain recommendations for hardware required for the proposed Management Group.

Demonstration: Using the System Center 2012 Operations Manager Sizing Helper Tool

In this demonstration, you learn how the System Center 2012 Operations Manager Sizing Helper is used to calculate the hardware requirements of an Operations Manager Management Group.

Demonstration Steps

1. To perform this task, use the computer and tool information provided in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Manager Sizing Helper Tool
Location	C
File	System Center 2012 Operations Manager Sizing Helper Tool v1.xls

2. Configure the **Standard Deployment** as follows:
 - a. APM: **Enabled**
 - b. Number of Server Computers: **400** in both sections.
 - c. Number of APM-enabled Computers: **50** in both sections.
 - d. Number of Network Devices: **120** in both sections.
 3. Review the properties of the **Minimum Hardware Recommendation** information.
- Question:** What TCP/IP port must be open between the Operations Manager agent and the Management Server that it reports to?

Lab: Using the System Center 2012 Operations Manager Sizing Helper Tool

Scenario

After you have gathered the relevant monitoring requirements for Contoso, Ltd., you must use the System Center 2012 Operations Manager Sizing Helper tool to determine the infrastructure that will be required to deploy the Operations Manager Management Group. Contoso's IT environment currently includes the following:

- 200 servers running Windows in a private cloud (including physical hosts)
- 50 servers running Windows in Microsoft Azure
- 50 servers running Windows in a trust boundary
- 100 servers running UNIX/Linux
- 50 line-of-business .NET-based and Java-based application servers
- 120 network devices

Keep in mind that the Management Group must have the following characteristics:

- High availability
- Scalability
- Fault tolerance

Objectives

After completing this lab, you will be able to:

- Use the System Center 2012 Operations Manager Sizing Helper tool to determine the infrastructure that will be required to deploy the Operations Manager Management Group into Contoso's IT environment.

Lab Setup

Estimated Time: 15 minutes

Virtual Machines: 10964C-LON-DC1, 10964C-LON-MS1

User Name: Contoso\Administrator

Password: Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:

- 10964C-LON-MS1



Note: Before you start this lab, make sure that all Windows Services that are set to start automatically are running, except for the Microsoft .NET Framework NGEN 4.0.30319_X86 and the.NET Framework NGEN 4.0.30319_X64 services, because these services stop automatically when they are not being used.

Exercise 1: Calculating the Hardware Requirements for Contoso's Management Group

Scenario

After you have determined both the number of computers and network devices to be monitored and the data retention requirements for the Contoso Management Group, you must use the System Center 2012 Operations Manager Sizing Helper tool to determine the recommended hardware requirements.

The main tasks for this exercise are as follows:

1. Configure the standard deployment values
2. Review the advanced deployment values
3. Configure the advanced database sizing values

► Task 1: Configure the standard deployment values

1. To configure the standard deployment values, use the computer and tool information provided in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Manager Sizing Helper Tool
Location	C
File	System Center 2012 Operations Manager Sizing Helper Tool v1.xls

2. Submit a default **Standard Deployment** scenario with **APM** enabled, and then in the **DB Size** and **DW Size** sections manually edit the values as follows.
 - a. Number of Server Computers: **400** in both sections
 - b. Number of APM-enabled Computers: **50** in both sections
 - c. Number of Network Devices: **120** in both sections
3. Review the properties of the **Minimum Hardware Recommendation** information.

► **Task 2: Review the advanced deployment values**

- To review the advanced deployment values, use the computer and tool information provided in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Manager Sizing Helper Tool
Location	C
File	System Center 2012 Operations Manager Sizing Helper Tool v1.xls

- Review the following **Advanced Deployment** information for:

- Gateway Server
- UNIX or Linux Monitoring
- URL Monitoring

► **Task 3: Configure the advanced database sizing values**

- To perform this task, use the computer and tool information provided in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Manager Sizing Helper Tool
Location	C
File	System Center 2012 Operations Manager Sizing Helper Tool v1.xls

- Configure the **DB Size Calculator** as follows:

- Number of Server Computers: **400**
- Number of Network Devices: **120**
- Number of APM-enabled Computers: **50**

- Note the **Total Size (GB)** and **Estimated IOPS** column for **1-500** agents values.

- Configure the **DW Size Calculator** as follows:

- Number of Server Computers: **400**
- Number of Network Devices: **120**
- Number of APM-enabled Computers: **50**

- Note the **Total Size (GB)** and **Estimated IOPS** column for **1-500** agents values.

- Configure the **DB DW Disk Calculator** as follows:

- a. Enter Estimated IOPS [From DBSize and DWSize TAB]: **750**
- b. Enter the Estimated Disk Space in GB [From DBSize & DWSize TAB]: **434.94**
7. Review the **Estimated # of RAID disks required** information.
8. Close the **System Center 2012 Operations Manager Sizing Helper Tool v1.xls** window and save the changes.

Results: After this exercise, you should have configured the System Center 2012 Operations Manager Sizing Helper tool with appropriate values to determine the hardware required for the Contoso Management Group.

Exercise 2: Creating a Visio Diagram of the Proposed Management Group Design

Scenario

With the hardware requirements and Operations Manager components calculated, you must now represent the proposed Management Group design in a Microsoft Visio diagram. This will be used to show how the architecture of the Management Group including the network topology, Operations Manager components and trust boundaries.

The main tasks for this exercise are as follows:

1. Import the Visio diagram
2. Include communication flow and TCP/IP ports

► Task 1: Import the Visio diagram

1. To perform this task, use the computer and tool information that is provided in the following table.

Location	Value
Computer	LON-MS1
Tool	Visio 2013
Diagram	Contoso Management Group.vsdx
Location	C:

2. Open the **Contoso Management Group.vsdx** Visio diagram and review the various Operations Manager components that have been added to it.

► **Task 2: Include communication flow and TCP/IP ports**

- To perform this task, use the computer and tool information that is provided in the following table.

Location	Value
Computer	LON-MS1
Tool	Visio 2013
Template	Network
Diagram	Basic Network Diagram

- On the **Home** tab in the **Tools** group, use the **Connector** option to create a connection between the following shapes, and then edit the text of the connections to display the following:
 - Connection from: Left **Management Server** shape
 - Connection to: **Operational database SQL Cluster**
 - Connection text: **1433**
 - Connection from: Right **Management Server** shape
 - Connection to: **Operational database SQL Cluster**
 - Connection text: **1433**
 - Connection from: Left **Management Server** shape
 - Connection to: **Data Warehouse and SSRS databases**
 - Connection text: **1433**
 - Connection from: Right **Management Server** shape
 - Connection to: **Data Warehouse and SSRS databases**
 - Connection text: **1433**
 - Connection from: **Reporting Server** shape
 - Connection to: Left and right **Management Server** shape
 - Connection text: **5723/5724**
 - Connection from: **Web Console Server** shape
 - Connection to: Left and right **Management Server** shape
 - Connection text: **5724**
 - Connection from: **Web Console** shape
 - Connection to: **Web Console Server**
 - Connection text: **80**
 - Connection from: **Operations Console** shape
 - Connection to: Left and right **Management Server** shape
 - Connection text: **5724**
 - Connection from: Top **Agent Managed Computers** shape

- Connection to: Left and right **Management Server** shape
- Connection text: **5723**
- Connection from: Bottom **Agent Managed Computers** shape
- Connection to: **Gateway Server**
- Connection text: **5723**
- Connection from: **Gateway Server** shape
- Connection to: Both **Management Server** shapes
- Connection text: **5723**

Results: After this exercise, you should have created a Visio diagram of the proposed Management Group design for Contoso.

Question: What is the core function of Management Servers in Operations Manager?

Module Review and Takeaways

Best Practices

 **Best Practice:** Resource pools provide a pool of Management Servers that can be used to provide failover for monitored network devices and UNIX-based and Linux-based computers. If a Management Server in the pool fails, the load is automatically distributed to other Management Servers in the pool. Scalability and resilience is provided by adding more Management Servers. Therefore, it is recommended that all Management Servers have no more than 5 milliseconds (ms) latency between them.

Review Question(s)

Question: What feature is provided when Operations Manager is integrated with System Center Advisor?

Real-world Issues and Scenarios

As part of your plan for an Operations Manager Management Group, you should review the TechNet article "Planning the System Center 2012 - Operations Manager Deployment," which can be found here:

<http://go.microsoft.com/fwlink/?LinkId=391264>

Tools

System Center 2012 Operations Manager Sizing Helper. This tool provides good hardware recommendations that are based on several factors such as the number of monitored computers and network devices. The tool can be downloaded from here:

<http://go.microsoft.com/fwlink/?LinkId=321884>

Module 2

Deploying a New System Center 2012 R2 Operations Manager Management Group

Contents:

Module Overview	2-1
Lesson 1: Overview of Security Considerations	2-3
Lesson 2: Designing the Management Group	2-6
Lesson 3: Installing System Center 2012 R2 Operations Manager	2-11
Lesson 4: Configuring Operations Manager Default Settings	2-17
Lesson 5: Deploying the Operations Manager Agent	2-21
Lesson 6: Configuring Agentless Exception Monitoring (AEM)	2-30
Lesson 7: Configuring Audit Collection Services	2-34
Lab: Installing System Center 2012 R2 Operations Manager and Deploying Agents	2-40
Module Review and Takeaways	2-63

Module Overview

When planning a new deployment of Microsoft System Center 2012 R2 Operations Manager, you should consider not only your hardware and sizing requirements, but also other factors, such as the security accounts that Operations Manager requires and the design of the Management Group. For example, you might have a requirement to install two separate Management Groups so that you can scale Operations Manager to meet your monitoring requirements.

After installing Operations Manager, you should also be aware of some of the most common settings that should be configured, such as data retention (database grooming) settings, and manual agent installation approval settings. You should also be aware of the agent deployment methods that are available and when to use them, including the console (or push) method and the manual installation method.

Objectives

After completing this module, students will be able to:

- Know the security considerations when deploying Operations Manager.
- Know the Management Group design considerations.
- Install System Center 2012 R2 Operations Manager.
- Configure common settings in System Center 2012 R2 Operations Manager.
- Configure Agentless Exception Monitoring in System Center 2012 R2 Operations Manager.
- Deploy agents in System Center 2012 R2 Operations Manager.

- Configure Audit Collection Services in System Center 2012 R2 Operations Manager.

Lesson 1

Overview of Security Considerations

When installing Operations Manager, you must supply the credentials for a number of security accounts that Operations Manager uses to perform many of its tasks, such as inserting data into the Operations Manager databases. It is important that you understand the requirements of these accounts, including the permissions that the accounts must have for the relevant Operations Manager component. In secure environments, such as where Active Directory Domain Services (AD DS) is locked down, you should also understand how the Health Service Lockdown tool (HSLockDown) can be used to control and limit health service access on domain controllers.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe the Operations Manager accounts, including the permissions required for each.
- Control and limit health service access on domain controllers by using HSLockDown.

Operations Manager Security Accounts

Operations Manager uses several service accounts that are configured either during the initial setup or during specific operations such as deploying agents. The following sections describe accounts and their use, and the account type that they can be configured with depending on your security policy.

Action Accounts

Action accounts in Operations Manager are used to perform monitoring tasks on managed computers. Action accounts run a process that can be identified as MonitoringHost.exe to perform

these tasks. Tasks include monitoring event logs and performance counters, collecting data for reports, and running scripts or batch files. An action account is associated with the Management Server, Agent, and Gateway Server. Action accounts can run under the context of a local system account or can be a domain or local user account. Typically, a domain account is used, because this lets you assign only the necessary permissions that are required. In a low-privilege scenario such as this, as a minimum, the following permissions should be assigned to action accounts:

- Member of the local Users group
- Member of the local Performance Monitor Users group
- Allow Log On Locally permission (SetInteractiveLogonRight)

Each Management Pack requires a specific set of permissions for it to perform the relevant tasks that it is designed for. Reviewing the Management Pack guide is recommended so that you can make sure the permissions are set appropriately, because there might be a requirement to configure a Run As Account in Operations Manager, which is used to perform the Management Pack tasks.

Operations Manager accounts:

- Action accounts
- System Center Configuration service and System Center Data Access service
- Data Writer account
- Data Reader account



System Center Configuration service and System Center Data Access service

This account is used to read and update data in the Operations Manager operational database. The account must have local administrative rights on the Management Server. You can use either a domain account or a local system account. A local system account, however, can be used only when the Operations Manager operational database is located on the same computer as the Management Server. Therefore, typically, it is used only in evaluation or test environments where all features are installed on the same computer.

A local user account is not supported for the Data Access Service and Configuration Service Account.

When you install multiple Management Servers, the account that is specified as the Data Access Service and Configuration Service Account should be the same for each Management Server installation. This is also the case with the account that is specified as the Management Server action account.

Data Writer Account

The Data Writer Account is used to collect data from the operational database and write data to the reporting data warehouse. During installation, the Data Writer Account is automatically assigned write permissions to the OperationsManagerDW database and is also assigned read permissions to the OperationsManager database. The account that is specified for the Data Writer Account must have Microsoft SQL Server logon rights and logon rights to the computer that is hosting the Operations Manager databases.

Data Reader Account

SQL Server Reporting Services (SSRS) uses the Data Reader Account to run queries against the Operations Manager reporting data warehouse. The account must be a domain account, and have Microsoft SQL Server logon rights and logon rights on the Management Server.

Overview of the HSLockdown Tool

In high-security-related environments such as an environment where payment card details are stored, the Health Service Lockdown (HSLockDown) tool might be required to control which security contexts the monitoringhost process can run under. The HealthService runs as localsystem, however, the workflows that it instantiates by default run under the default action account.

The HSLockDown tool is used to control under which accounts the HealthService can instantiate workflows. There are three scenarios in which you might need to use the HSLockDown tool:

- You want to explicitly deny the agent the ability to run rules, tasks, and monitors as a specific account (such as local system).
- You configured the agent to not run as local system but did not configure a Privileged Monitoring Account.
- The target machine has a security policy that explicitly denies the agent from instantiating monitoringhost processes under a different security context.

The HSLockDown tool is used to control access to the Health Service and has the following four switches:

- L** - List accounts/groups
- A** - Add an allowed account or group
- D** - Add a denied account or group
- R** - Remove an allowed/denied account or group

To use the HSLockdown tool, at a command prompt, run the HSLockdown command from the folder where the Operations Manager media is installed. This is typically \Program Files\Microsoft System Center 2012 R2\Operations Manager\Server on a Management Server, and \Program Files\Microsoft Monitoring

Agent\Agent on an agent-managed computer. When using the tool, you can use any of the following four switches to control access to the Health Service:

- **HSLockdown [ManagementGroupName] /L - List Accounts/groups**
- **HSLockdown [ManagementGroupName] /A - Add an allowed account|group**
- **HSLockdown [ManagementGroupName] /D - Add a denied account|group**
- **HSLockdown [ManagementGroupName] /R - Remove an allowed/denied account|group**

As an example, the following command would be used to remove the NT AUTHORITY\SYSTEM account from the deny list.

```
hslockdown "Management_Group _Name" /R "NT AUTHORITY\SYSTEM"
```

For more information about the HSLockdown tool visit the following website.



Control Access by Using the Health Service Lockdown Tool in Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=404082>

Question: In a low-privileged scenario, what are the minimum permissions that an action account should have?

Lesson 2

Designing the Management Group

Before you deploy an Operations Manager Management Group, you should consider the environment in which it will be installed. This will assist you in designing your Management Group, including the physical location of specific Operations Manager roles such as Management Servers and Gateway Servers.

Depending on the environment you are deploying, Operations Manager might require installation of multiple Operations Manager Management Groups. For example, there might be a requirement to separate monitoring data between environments such as development and production. This can also be the case in very large environments where the number of computers and devices to be monitored exceeds the monitoring capacity of a Management Group. In these scenarios, it is important to understand how data can be shared between Management Groups.

Lesson Objectives

After completing this lesson, students will be able to:

- Design the Management Group.
- Configure connected Management Groups in Operations Manager.
- Share alerts and tasks between a local and connected Management Group.
- Configure connected Management Groups across a trust boundary.

Management Group Design

In addition to the considerations such as hardware and software requirements, which were discussed in Module 1, “Overview and Architecture,” you should also consider the environment in which you will be deploying your Operations Manager Management Group. If the environment to be managed is spread across multiple geographical locations, for example, it is important to understand in which location each Operations Manager role is deployed. Described in the following sections are the factors that should be considered when deploying Operations Manager in both single and multiple datacenter environments.

When designing an Operations Manager Management Group, you should consider:

- Number of agent-managed computers
- Number of network devices
- Trust boundaries
- Network latency
- High availability



Single Datacenter Environment

In a single datacenter environment where there is little or no network latency, all Operations Manager roles will be able to communicate with each other without any delay or interruption. Factors that should be considered include:

- **How many computers are to be managed.** This will directly affect the sizing of the Operations Manager databases and the number of Management Servers required.
- **How many network devices are to be managed.** This will also affect the sizing of the Operations Manager databases but might also affect the number of Management Servers. It is recommended for network device monitoring that a dedicated resource pool be used.

- **Monitoring across trust boundaries.** If there are untrusted domains that include computers to be managed, gateway servers can be deployed into these domains to manage them.
- **High Availability.** SQL Server Failover clustering can be implemented for the Operations Manager databases. Deploying multiple Management Servers will provide failover and load balancing and will also allow for continuous monitoring in the event of a failed Management Server.

Multiple Datacenter Environment

If the environment to be monitored spans multiple datacenters, you must consider several additional factors, such as the following:

- **Network latency.** If you need to monitor computers or devices in a remote location (or site), you should consider using Gateway Servers instead of Management Servers. With the introduction of resource pools, all Management Servers must be connected over a low-latency network. If you have Management Servers in the local site, and Management Servers in a remote site, it is recommended that all Management Servers be moved to the same datacenter and that you deploy Gateway Servers in the remote sites instead.
- **Location of the operational and data warehouse database servers.** Because Management Servers require a direct connection to the Operational and Data Warehouse database servers, it is important that the connection between them is over a low-latency network. In locations where the computers to be managed are in a high-latency network, use Gateway Servers to manage them.
- **Multisite failover.** If you require high-availability between sites in your Operations Manager environment, you have a number of options available to you. These include features such as SQL Log Shipping, SQL Server 2012 AlwaysOn: Multisite Failover Cluster, and multiple Management Groups, where a Management Group is installed in both sites and multihome agent-managed computers report to both Management Groups. Note that because of network latency, this last option might not always be viable. Configuring SQL Server 2012 AlwaysOn: Multisite Failover Clustering is discussed in detail later in this course.

Irrespective of the environment in which you deploy Operations Manager, you should also be aware of the **Minimum Network Connectivity Speeds** and **Monitored Item Capacity** supported by Operations Manager. As an example of **Minimum Network Connectivity Speeds**, communications between an agent and its associated management server must occur using a network connection speed of at least 64 Kbps. As an example of **Monitored Item Capacity**, a management server can manage up to 3,000 agent-managed computers and up to 10 agentless-managed computers.

For more information on **Minimum Network Connectivity Speeds** and **Monitored Item Capacity** in Operations Manager visit the following webpage.

Preparing your environment for System Center 2012 R2 Operations Manager

<http://go.microsoft.com/fwlink/?LinkID=391268>

Connected Management Groups

As described in Module 1, "Overview and Architecture," the various Operations Manager components such as the Management Servers, Gateway Servers, and Operations Manager databases form a Management Group. Where two or more Management Groups have been deployed, you can connect them and have them share information such as alerts and tasks. This allows a single Operations Manager console to be used to manage alerts from multiple Operations Manager environments. You might decide to deploy multiple Management Groups for a number of reasons, such as:

- You need a development environment to test developed Management Packs.
- For security reasons, you must separate data collected in one environment from data collected in another environment.
- You need to support an environment where more than 6,000 agents will be deployed.
- You need to consolidate monitoring across a trust boundary.

Connected Management Groups in Operations Manager provide a way to:

- View and interact with alert information from multiple Management Groups from within a single Operations Manager console



- Manage alerts from multiple Management Groups
- Run tasks on computers managed in connected Management Groups

When two or more Management Groups are connected, the Management Group to which other Management Groups connect is referred to as the *local Management Group*. The Management Groups that connect to the local Management Group are referred to as *connected Management Groups*. This is important to understand when designing your Management Group hierarchy, because only the local Management Group will display alerting information for connected Management Groups. Connected Management Groups share information only with the local Management Group they are connected to. They do not share information with other connected Management Groups.

You also need to take into account additional considerations when deciding to connect Management Groups:

- A Management Group cannot be a local and connected Management Group at the same time.
- The local and connected Management Groups must be running the same version of Operations Manager.
- Communication on ports 5723 and 5724 must be enabled between Management Servers in both the local and connected Management Group.

Before you add a Management Group to a local Management Group, you must also ensure the following:

- The Management Servers from both Management Groups must be able to resolve each other by using a Fully Qualified Domain Name (FQDN). If the Management Groups do not use the same Domain Name System (DNS) service, you might need to add a secondary DNS zone in the local Management Groups' DNS service, which will transfer the DNS information from the Primary zone in the DNS service used by the connected Management Group.
- The System Center Data Access Service and System Center Management Configuration Service account of the local Management Group must be added to the Operations Manager Administrators user role in the connected Management Group.
- For operators in the local Management Group to access data in the connected Management Group, you should identify the user names that exist in the local Management Group domain.

Connecting a Management Group

To connect a Management Group, you should perform the following tasks in the Operations console when it is opened as an Operations Manager Administrator:

1. From the **Administration** pane, right-click **Connected Management Groups**, and then click **Add Management Group**.
2. In the **Add Management Group** dialog box that opens, add the following information:
 1. The **Management Group name** that is to be connected.
 2. The FQDN of a **Management Server** in the Management Group to be connected.
 3. The account that will be used for the initial connection to the Management Group to be connected. You can either use the **Use SDK service account** option or the **Other user account** option, where you can add an account that is a member of the Operations Manager Administrators role for the connected Management Group.
4. Click **Add**.

The Management Groups are then connected, and the connected Management Group is displayed in the Results pane in the Connected Management Groups view.

Shared Alerts and Tasks Between a Local and Connected Management Group

After connecting a Management Group to a local Management Group, you must configure access to the alerts and tasks in the connected Management Group. Operations Manager user roles provides the mechanism for achieving this. First, you add to the relevant user role in the connected Management Group the users for whom you need to grant access. Then, in the local Management Group, you edit the relevant user role that contains the users to whom you are granting access. On the Group Scope tab, you select the connected Management Groups to which those users should have access.

You can configure access to a connected Management Group by:

- Adding users to the User Roles in the connected Management Groups
- Editing the User Roles in the Local Management Group and selecting the connected Management Groups
- Use the Show Connected Alerts button from the toolbar



When a user of the relevant user role opens any alert view in the Operations console, a Show Connected Alerts button becomes available in the toolbar. The user can click this to show alerts from the connected Management Groups to which they have been granted access.

After clicking the Show Connected Alerts button on the toolbar, the user is prompted for credentials to connect to the connected Management Group. The user must log on to the connected Management Group before any alerts are displayed.

Tasks for managed computers in the connected Management Group can also be performed from the Operations console in the local Management Group.

Connected Management Groups Across a Trust Boundary

If the local Management Group and Management Group to be connected span a trust boundary, it is important that you understand how you can still consolidate alerts between the local and connected Management Group.

In this scenario, for users in the local Management Group to authenticate to the connected Management Group, you must create associated user accounts in the connected Management Group domain and then add them to the relevant Operations Manager user roles. When users from the local Management Group connect to the connected Management Group, they use these credentials to connect.

Remember that if a firewall separates the domains, TCP ports 5723 and 5724 must be opened for the Management Servers from both Management Groups to communicate. In addition, DNS resolution must be configured such that the Management Server in the connected Management Group can be resolved by using a FQDN.

To add a connected Management Group in an untrusted domain, you must:

1. Ensure port 5723 and port 5724 are open between the Management Servers in both Management Groups
2. Ensure the Management Server in the connected Management Group can be resolved by FQDN from the local Management Group
3. Create user accounts in the untrusted domain and add them to the relevant user roles
4. Use these accounts when connecting to the connected Management Group from the local Management Group

Question: You need to connect a local Management Group running Microsoft System Center Operations Manager 2007 R2 to another Management Group running System Center 2012 R2 Operations Manager. What is the first task you should perform?

Lesson 3

Installing System Center 2012 R2 Operations Manager

After you have completed your Operations Manager design and have provisioned the underlying infrastructure for the Operations Manager Management Group or Groups, you can then deploy Operations Manager. It is important that you understand the procedure for deploying Operations Manager, including the order in which each component is installed. This procedure will differ depending on factors such as whether you are deploying a single or distributed Operations Manager Management Group.

Lesson Objectives

After completing this lesson, students will be able to:

- Install a distributed System Center 2012 R2 Operations Manager Management Group.
- Confirm the Management Group is operating as expected.

Installation of a Distributed System Center 2012 R2 Operations Manager Management Group

In a distributed deployment of Operations Manager, you run Setup.exe from the Operations Manager media, and then install each Operations Manager feature on the server that you have provisioned for the feature being installed. There is a specific installation order that should be followed when you install each feature in a distributed deployment of Operations Manager. For example, you cannot install the Reporting Server feature until the first Management Server has been deployed. Described in the following table are the high-level steps to perform when deploying a distributed Operations Manager Management Group.

A typical deployment of a distributed Operations Manager Management Group includes:

- Management Servers, including the Operations Manager databases
- Operations console
- Reporting Server
- Web console
- Gateway Server



Installation Step	Description
1. Install the first Management Server	<p>During the installation of the first Management Server, both the operational database and data warehouse database are created on the specified SQL Server while working through the setup wizard. You also specify a name for the new Management Group and supply the account credentials for the following Operations Manager accounts:</p> <ul style="list-style-type: none"> • Management Server action account • System Center Configuration service and System Center Data Access service • Data Reader account • Data Writer account <p>You can also install an Operations console during this step.</p>
2. Install additional Management Servers	<p>At least two Management Servers in any Management Group is recommended. This allows for failover and load balancing. During the installation of an additional Management Server, you select Add A Management Server To An Existing Management Group, and then specify the computer name of the SQL Server that hosts the Operations Manager database. You also supply the account credentials for the following Operations Manager accounts:</p> <ul style="list-style-type: none"> • Management Server action account • System Center Configuration service and System Center Data Access service account <p>The credentials specified here must be the same credentials that were specified when installing the first Management Server.</p> <p>You can also install an Operations console during this step.</p>
3. Install the Operations console	<p>Although you can install the Operations console when installing a Management Server, you might also need to install just the Operations console, for example, on a workstation computer. After installing the Operations console, a Connect To Server page is displayed in which you specify the computer name of the first Management Server that was installed. The Operations console then opens.</p>
4. Install the Operations Manager Reporting Server	<p>During the installation of the Reporting Server, you must specify a Management Server that will be used by the reporting feature only. You also select the SQL Server instance that hosts SSRS. Note that SSRS must be installed locally on the computer that will host the Operations Manager Reporting Server. The SSRS databases (ReportServer and ReportServerTempDB), however, can be installed on a remote SQL Server. You must also supply the credentials for the Data Reader account.</p>
5. Install the Operations Manager Web console	<p>The Web console can be installed on an existing Management Server, or it can be installed separately. It should be noted, however, that you cannot add the Management Server feature to a computer that already hosts a Web console. When installing the Web console, the Application Diagnostics and Application Advisor consoles are also installed. These consoles cannot be installed separately. During the installation of the Web console, you specify the computer name of a Management Server that only the Web console uses. Also, you select either the Default Web Site or an existing website in which the Web console will be installed, and also specify if Secure Sockets Layer (SSL) should be enabled to provide secure communication to the Web console. Additionally, you specify the authentication mode for use with the Web console, such as Mixed Authentication or Network Authentication. Mixed Authentication is used in intranet environments, and Network Authentication is used in extranet environments.</p>
6. Installing a	<p>If you need to manage a number of computers that reside in an untrusted</p>

Installation Step	Description
Gateway Server	<p>domain, you can use the Gateway Server feature. The Gateway Server is installed in the untrusted domain and uses a certificate to communicate securely with one or more Management Servers in the trusted domain. Agent-managed computers in the untrusted domain send collected data to the Gateway Server instead of to a Management Server. Before installing the Gateway Server, you should perform the following prerequisite steps:</p> <ul style="list-style-type: none"> • Request certificates for the Gateway Server and Management Server. • Import the certificates by using the MOMCertImport.exe tool. • Copy Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to the Management Server. • Run Microsoft.EnterpriseManagement.GatewayApprovalTool.exe to configure communication between the Gateway Server and the Management Server. <p> Note: These steps are covered in detail later in this module in the Lab, "During the installation of the Gateway Server, you specify the computer name of the Management Server to which the Gateway Server will communicate. You specify the Management Group name. By default, communication between the Gateway Server and Management Server uses TCP Port 5723, although if configured in the Operations console, a different port can be specified. You also specify the account credentials that will be used as the Gateway action account. A Local System, Local Computer, or Domain account can be used here. If a Gateway Server is not used in the untrusted domain, every computer that must be monitored will need to have a certificate installed to communicate securely with the Management Server or Servers in the trusted domain. For this reason (and to reduce administration overhead), in scenarios where there are more than five computers to be managed in an untrusted domain, a Gateway Server should be used. Note that the Gateway Server is often used to replace a Management Server in locations over a slow wide area network (WAN) link. In this scenario, certificates are not required. It should also be noted that multiple Gateway Servers can be installed to provide load balancing and failover capabilities for agent-managed computers. Similarly, Gateway Servers can be configured to failover to other Management Servers in the Management Group should their primary Management Server fail."</p>
7. Installing Audit Collection Services	Audit Collection Services (ACS) is covered later in this module in the lesson titled "Configuring Audit Collection Services."

The preceding table describes the core components that are installed when deploying a distributed Operations Manager Management Group. Other components such Agentless Exception Monitoring can be enabled as required.

 **Note:** You can also install Operations Manager features by using a Command Prompt window. The following command uses Setup.exe from the Operations Manager media to install all core components of Operations Manager (note the /components switch that is being used):

```
setup.exe /silent /install
/components:OMServer,OMConsole,OMWebConsole,OMReporting
/ManagementGroupName: "<ManagementGroupName>"
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DWDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
```

```

/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/AcceptEndUserLicenseAgreement: [0|1]
/WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]
/WebConsoleAuthorizationMode: [Mixed|Network]
/SRSInstance: <server\instance>
/SendODRReports: [0|1]
/EnableErrorReporting: [Never|Queued|Always]
/SendCEIPReports: [0|1]
/UseMicrosoftUpdate: [0|1]

```

Methods for Confirming Successful Deployment of a Management Group

After deploying the Management Group, you can confirm it is in a healthy state by using various views and reports that are available within the Operations console. Described in the following sections are some of the common views and reports that can be used to check the health of an Operations Manager Management Group.

Distributed Applications View

One of the first (and most useful) views to open when monitoring the health of the Operations Manager Management Group is the Operations Manager Management Group distributed application diagram. This can be opened from the Distributed Applications view in the Monitoring pane. After opening the view, you can instantly see the health of all Operations Manager components, such as the Operational and Data Warehouse databases, health services, Web consoles, and report console in a single pane. If any component is in an unhealthy state, it will be shown here in either a yellow (warning) or red (critical) state. You can then use the health explorer to determine the cause of the unhealthy state. Distributed Application Diagrams are covered in greater detail later in this course.

To help confirm the **health state** of a Management Group, you can use the following views:



- Distributed Applications view
- Active Alerts view
- Operation Manager views
- Management Servers view
- Most Common Alerts report

Active Alerts View

Any issues that have been detected in the Management Group will result in an alert being generated in the Active Alerts view of the Monitoring pane. Although the Active Alerts view displays alerts for all applications and services monitored by Operations Manager any Management Group, related alerts will also be displayed here. When opening an alert, the General and Product Knowledge tabs can be used to obtain detailed information about the alert, including possible resolution steps.

Operations Manager Views

Within the Operations Manager folder in the Monitoring pane are a number of views that can be used to determine the performance and availability of the Management Group. For example, the Management Group Health dashboard provides a single view that displays the health state of each Management Group function such as the Web User Interfaces, All Management Servers Resource Pool, and Data Access Service Group. Included in the dashboard is the health state for the Management Group Infrastructure components such as the Data Warehouse Database, Operations Database, and Operations Manager Management Servers. The dashboard also includes active alerts relating to the Management Group. The Management Group Health dashboard is very useful in getting an overall view of the health of the Management Group because it displays all of the aforementioned information in a single view.

Management Servers View

In the Administration pane, the Management Servers view from within the Device Management node displays the health state for all Management Servers and Gateway Servers in the Management Group. If the health state for any server is in a critical or warning state, you can right-click the server and open related views such as the Alert view or Event view. This is useful, because you can quickly obtain context-sensitive information without needing to browse to another area of the console. Similar views such as the Agent Managed and UNIX/Linux Computers views are also available from within the Device Management node.

Most Common Alerts Report

The Most Common Alerts report that is available in the Microsoft Generic Report Library folder in the Reporting pane can be used to provide a report of common or reoccurring alerts within the Management Group. This can be useful in knowing where to concentrate your troubleshooting. You can filter the report based on the Management Pack, such as the Data Warehouse Library or Health Library Management Pack. This helps by removing alerts from the report that you do not need to review.

When you have installed Management Packs such as the Windows Operating System, SQL Server, and Microsoft Internet Information Services (IIS) Management Packs, other views and reports become available and provide performance, health, and availability metrics for the Management Group components.

Using a combination of the views and reports described, you can quickly determine the health state of the Operations Manager Management Group and confirm it is operating as expected.

Demonstration: Installing System Center 2012 R2 Operations Manager

In this demonstration, you will learn how to install a Management Server in a new System Center 2012 R2 Operations Manager Management Group.

Demonstration Steps

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-SC1
Tool	Operations Manager Setup
Location	\LON-DC1\Media \LON-DC1\Media\SCOM2012R2
Setup file	Setup.exe

2. Install **ReportViewer** by using default settings.
3. Install Operations **Manager** by using the following settings (all other settings should remain the default):
 - Features to install: **Management Server** and **Operations Console**
 - Management Group name: **DEMO**
 - Operational Database name: **DemoDB**
 - Data Warehouse Database name: **DemoDWDB**
 - Server name and instance name: **LON-SQ1**

4. Configure Operations Manager Accounts:

Account name	Domain\user name	Password
Management server action account	Contoso\svc_SCOM2012_msaa	Pa\$\$w0rd
System Center Configuration service and System Center Data Access service	Contoso\Administrator	Pa\$\$w0rd
Data Reader account	Contoso\svc_SCOM2012_dwread	Pa\$\$w0rd
Data Writer account	Contoso\svc_SCOM2012_dwwrite	Pa\$\$w0rd

Question: When installing the Web console server, what three consoles are installed?

Lesson 4

Configuring Operations Manager Default Settings

After you complete the deployment of Operations Manager, a number of settings are typically configured in the Operations console. Settings include the data retention for the Operations Manager operational database, and the review manual agent installation setting. It is important that you understand how to configure these settings because they affect the size of the Operations Manager operational database and how manually installed agents are treated in Operations Manager.

Lesson Objectives

After completing this lesson, students will be able to:

- Configure data retention in Operations Manager.
- Enable manual agent installations in Operations Manager.
- Configure automatic alert resolution.

Data Retention

Operations Manager collects data for monitoring and reporting purposes and stores this data in both the Operational and Data Warehouse SQL Server databases. As with any application that uses SQL Server, it is important that the database size is maintained. This not only ensures that the application using the data is responsive at all times but also helps keep backup sizes to a minimum. Data retention in the Data Warehouse database is covered later in this course. Here you will learn how to configure data retention in the Operational database.

Database grooming can be configured for the following data types:

- Resolved alerts
- Event data
- Performance data
- Task history
- Monitoring job data
- Availability history
- State change events data
- Performance signature
- Maintenance mode history

As alluded to above, keeping the Operational database size to a minimum in Operations Manager helps keep the Management Group performing well. Although there are maintenance tasks run against the database to help ensure it is always available and performing, you should also configure the data retention settings such that only the data you need to keep is retained in the Operational database.

In the following table, the data that Operations Manager collects and stores in the Operational database is provided, including the default data retention settings for each data type:

Data type that Operations Manager collects	Default data retention (days)
Resolved alerts	7
Event data	7
Performance data	7
Task history	7
Monitoring job data	7

Data type that Operations Manager collects	Default data retention (days)
State change events data	7
Performance signature	2
Maintenance mode history	7
Availability history	7

By default, when data becomes older than specified in the preceding table, it is removed from the Operational database. This process is known as *database grooming*.

You can change the default data retention settings in Operations Manager to suit your needs. For example, you might need to retain Resolved Alert data for only three days and Availability history data for four days. To change the data retention settings, you edit the properties of the Database Grooming setting in the Settings node in the Administration pane of the Operations console.

You can edit each data type's setting from the Database Grooming setting and then set the desired data retention. It is recommended that you keep the data retention settings to a minimum to improve the performance of the Operational database, which in turn improves the performance of the overall Management Group.



Note: It is not possible to configure data retention for the Operations Manager data warehouse database using the Operations console. Instead, you must either use SQL Server Management Studio or the DWDataRP.exe utility. These methods are described later in this course.



Note: You can also configure data retention for the operational database by using the Set-SCOMDatabaseGroomingSetting PowerShell Cmdlet. The following example sets the number of days in which resolved alerts are kept to 25:

```
Set-SCOMDatabaseGroomingSetting -AlertDaysToKeep 25
```

Manual Agent Installation Settings

Installing agents in Operations Manager is covered later in this module. However, one important setting must be configured in Operations Manager before manually installed agents can communicate with the Management Group and send monitored data back to their assigned Management Server.

By default, Operations Manager rejects manually installed agents. This is a security feature. Until the Review New Manual Agent Installations In Pending Management View option is enabled, any manually installed agents are not visible in the console. A manually installed agent must be visible in the console for an operator to approve it.

Before manually installed agents can communicate with the Management Group:

- You must enable the **Review New Manual Agent Installations In Pending Management View** option
- You can enable this option for the whole Management Group or for a specific Management Server

You can enable the Review New Manual Agent Installations In Pending Management View option globally for all Management Servers by using the Security settings in the Administration pane. You can also enable it for each Management Server separately. Do this by enabling the setting in the Security tab while editing the properties of a Management Server in the Management Servers view of the Device Management node in the Administration pane.

If an agent is installed manually and has not been authorized to communicate with the Management Group, the Operations Manager event log on the agent-managed computer reports an Error event with an event ID of 21016. The description of the event states that "OpsMgr was unable to set up a communications channel to <ManagementServerName> and there are no failover hosts." Also, the Operations Manager event log on the Management Server states that the agent is designated as its primary and displays event ID 20000. This event ID notifies you that the principle name of the agent is trying to communicate to the Management Server and that it is probably not authorized.

With the Review New Manual Agent Installations In Pending Management View setting enabled, the Operations Manager agent is displayed in the Pending Management view of the Device Management node in the Administration pane. Before monitoring starts, you must approve the agent by using the Approve task when you select an agent in the Pending Management view.

Although not recommended, you can also configure Operations Manager to automatically approve manually installed agents by selecting the Automatically Approve New Manually Installed Agents check box after selecting the Review New Manual Agent Installations In Pending Management View option.

Automatic Alert Resolution

Another common setting that is customized after installing Operations Manager is the Automatic Alert Resolution setting. This setting determines how many days an alert in the New resolution state remains active before it is automatically resolved. You can also configure alerts to be automatically resolved when the alert source remains in a healthy state for a specific number of days.

By default, active alerts that are in a New resolution state and have not been updated for more than 30 days are automatically resolved.

Active alerts where the alert source has remained healthy for over 7 days are also automatically resolved by default.

To modify these settings, you edit the properties of the Alerts setting in the Settings node of the Administration pane. On the Automatic Alert Resolution tab, you can modify the Resolve All Alerts In The New Resolution State After and Resolve All Active Alerts When The Alert Source Is Healthy After settings to suit your automatic alert resolution needs.

Keeping these settings to a minimum can also help reduce the Operational database size, because alerts are automatically resolved as part of the database grooming process, as described in the "Data Retention" topic earlier in this lesson.

Alert Resolution States are also configured by using the Alerts setting and are described in detail later in this course.

Automatic alert resolution provides a method of automatically resolving alerts when:

- They are in a new resolution state for more than x number of days
- The alert source remains healthy for more than x number of days





Note: You can also configure automatic alert resolution settings by using the SCOMAlertResolutionSetting PowerShell Cmdlet. The following example configures the alert resolution settings so that active alerts are automatically resolved after 15 days, and active alerts are automatically resolved when the alert source has been healthy for 10 days:

```
Set-SCOMAlertResolutionSetting -AlertAutoResolveDays 15 -HealthyAlertAutoResolveDays  
10
```

Question: You need to reduce the amount of data retained in the Operations Manager operational database such that only three days of Event Data is retained. What should you do?

Lesson 5

Deploying the Operations Manager Agent

Before you can start to monitor your applications and services by using Operations Manager, you must deploy an agent to the computers that host them. Agent deployment in Operations Manager can be performed by using a number of different methods. Deciding which is the best method will depend on factors such as the location of the computers, their security context, and the number of agents to be deployed.

There are two methods of deploying agents in Operations Manager. These are Console (or push), and Manual. Typically the push method is used when there are a large number of agents to be deployed at one time. Manual installations typically occur when the computer to which the agent is to be deployed does not reside within the same or trusted domain as the Operations Manager Management Group.

Operations Manager also has the ability to use AD DS to automatically assign agents to a Management Group, which is useful where an automated build or scripted installation is preferred.

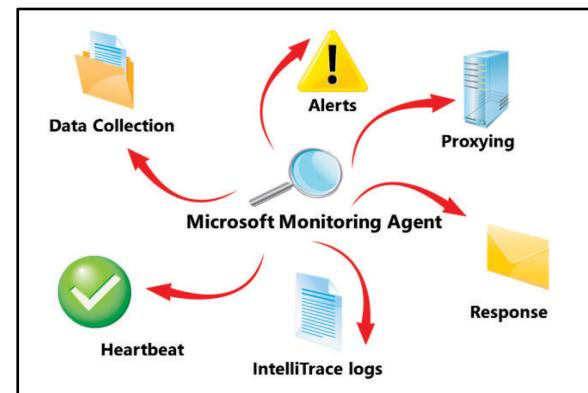
Lesson Objectives

After completing this lesson, students will be able to:

- Describe the Microsoft Monitoring Agent in System Center 2012 R2 Operations Manager.
- Use the Operations console to deploy an Operations Manager agent.
- Manually install an Operations Manager agent.
- Enable Active Directory Integration by using Operations Manager.

Overview of the Microsoft Monitoring Agent

The Microsoft Monitoring Agent in System Center 2012 R2 Operations Manager replaces the Operations Manager Agent and provides additional functionality such as the Microsoft IntelliTrace feature found in Microsoft Visual Studio development system. With IntelliTrace, full application-profiling traces can be collected from Microsoft .NET applications monitored with APM. This feature can be enabled on demand or can be enabled and left running to collect traces over a period of time.



The Microsoft Monitoring Agent can be deployed as part of an Operations Manager Management Group or can be installed separately to monitor .NET web applications. The trace logs that are collected by IntelliTrace can then be opened in Visual Studio Ultimate. IntelliTrace is covered in greater detail later in this course.

In addition to the new features previously listed, the Microsoft Monitoring Agent still provides the core monitoring functionality provided in previous Operations Manager Agents. Detailed in the following sections are some of the key monitoring features that the Microsoft Monitoring Agent provides.

Data Collection

One of the key functions that the agent provides is collecting data. Based on configuration from Management Packs that have been deployed in Operations Manager, the agent collects performance and monitoring data for applications and services running on the computer on which it is installed. This data is then compared with values configured in Management Packs to determine when thresholds are breached. For example a Management Pack might include a monitor to check the health state of the local system disk. The monitor might dictate that when the amount of available disk space falls below five percent, the health state of the system disk should change to critical. It is the agent's job to determine the amount of available disk space and then to report this information back to the Management Server to which it is associated.

Alerts

When an agent determines that a threshold has been breached, it can generate an alert that is represented in the Operations console. This is primarily how operators are notified of a problem. Other notification methods such as email or Short Message Service (SMS) can also be used.

Responses

Agents can also perform responses on the managed computer on which it is installed. This could include tasks such as clearing a temp folder or restarting a failed service. These tasks could be created by using a number of different methods such as a Microsoft Visual Basic script (VBScript) file or a batch file. The responses form part of the Management Packs that are distributed based on applications that have been discovered.

Heartbeats

For agents to collect data and send alert information back to their assigned Management Server, they must be available at all times. If communication between an agent and its Management Server fails, the agent will continue to collect performance and monitoring data on the managed computer but will not be able to generate alerts until communication is restored. For this reason, the agent also sends a packet of data every 60 seconds (by default) to its Management Server. This is known as a *heartbeat* and is used to determine the availability of the agent on a managed computer. If a heartbeat is not received within this timeframe, an alert is generated in the Operations console.

Proxying

By default, Operations Manager prohibits agents from sending data about other entities. This is a security restriction to stop agent spoofing. However, under some circumstances, it is desirable to enable this behavior. The most common scenario in which you would want to enable this behavior is monitoring of clusters. The cluster nodes are machines that collect and report on data relating to the virtual node.

Agents can also be used to collect monitoring data for computers or devices where an agent cannot be installed. This could be the case in scenarios where a computer cannot host an Operations Manager agent, such as in a highly secure environment. When deploying the agent, you can choose the Agentless option. In this scenario, a proxy agent is selected that will collect monitoring data on the computer's behalf. Note that not all Management Packs support agentless monitoring. The Management Pack guide that comes with each Management Pack should be reviewed to determine agentless compatibility. Both agents and Management Servers can be configured for proxying. To enable proxying, select the Allow This Server To Act As A Proxy And Discover Managed Objects On Other Computers check box on the Security tab when editing the properties of a Management Server or agent.

Note also that agentless monitoring is not the same as AEM, which is used to collect application and operating system exception errors, as described earlier.

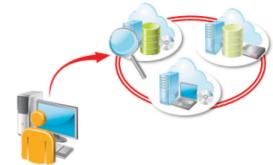
Console (Push) Deployment

The Console (or push) method of deploying the Operations Manager agent is the simplest and easiest method. The Discovery Wizard in the Operations console provides several discovery methods that you can use to find computers on the network. Agents that are deployed by using the Discovery Wizard can also be managed by using the Operations console for tasks such as agent version updates, and Management Server assignment.

Described in the following table are the pages of the Discovery Wizard, including the options that are available when you deploy an agent to a Windows-based computer.

Using the Discovery Wizard, you specify:

- Discovery type
- Auto or advanced discovery
- Discovery method
- Administrator account
- Computers to manage



Discovery Wizard page	Description
Discovery Type	On this page, you specify the type of computers or devices to manage. Options are Windows Computers (the default setting), UNIX/Linux Computers, or Network Devices.
Auto or Advanced	On this page, you decide the discovery type to use to discover the Windows-based computers. Automatic Computer Discovery scans the current domain and returns a list of computers that do not already have the Operations Manager agent installed. This is where you select the computers on which the agent should be deployed. Advanced Discovery (the default setting) lets you specify the computer type, such as Server And Clients, Servers Only, or Clients Only. This setting is useful, for example, if you must discover only servers. This action increases scanning speed when a scan of a Domain is performed. You also specify the Management Server or Gateway Server to which the agent will be assigned.
Discovery Method	When you select the Advanced Discovery type on the previous page, you specify how Operations Manager discovers the computers. The Scan Active Directory method (the default setting) lets you select the domain to scan. Then you build a Lightweight Directory Access Protocol (LDAP) query by using Active Directory object names, such as computer name and owner. This is useful when there are several computers on which you must install the Operations Manager agent, and these computers follow a naming standard. For example, there might be two computers, one with the computer name of LON-DC1 and the other with the name of LON-DC2. By using *DC* as the computer name to search, Operations Manager automatically discovers both computers. Using the browse method, in which you enter the computer names, you can browse AD DS for computers. This method opens a Select Computer dialog box that resembles the dialog box displayed when using the Find option in Active Directory Users And Computers. In the Select Computer dialog box, you can search for computers in AD DS. Instead of browsing for computers, you enter the computer names, and then separate them with a comma, semicolon, or new line.
Administrator Account	On this page, you specify the administrator account that you will use to discover and install the agent on the selected computers. By default, Operations Manager will use the Management Server action account. The account that is specified here must have local administrative rights on the computer on which the agent is to be installed. Optionally, you can

Discovery Wizard page	Description
	<p>click the Other user account setting, where you manually enter the user name and password, and then select the domain in which the account resides. This account is then used to discover the computer and install the agent. This setting is especially useful in high-security environments, such as those in which you deploy agents to domain controllers or computers that host business-critical applications such as SQL Server. For example, a domain administrator or SQL database administrator (DBA) can use the console at this point to enter the relevant credentials without the Operations Manager administrator viewing them.</p> <p>During agent deployment, the credentials are encrypted and then discarded after the agent is installed. Optionally, you can select the This Is A Local Computer Account, Not A Domain Account check box. By using this option, you can specify a local computer account to install the agent. When you use this option, the discovery of the computers is performed by the Management Server action account.</p>
Select Objects to Manage	<p>Based on the discovery type and method setting, this page displays a list of discovered computers that you can manage. The list does not display computers that already have the Operations Manager agent installed.</p> <p>You select the computers on which to install the agent and optionally change the Management Mode. By default, the Management Mode is set to Agent. This means an agent will be installed on the selected computers. You can change this setting to Agentless, in which case, an agent is not installed.</p> <p>Be aware that not all Management Packs support the Agentless feature. For example, the Active Directory and Exchange Management Packs do not support agentless monitoring. Typically, only performance and availability data is collected from an agentless managed computer.</p> <p>When you select agentless, you also specify a proxy agent that will be used to provide remote agent functionality. You can use either a Management Server or agent-managed computer as the Proxy Agent.</p> <p>It is best practice to use an agent-managed computer as the proxy agent because of the additional resources that are required in monitoring an agentless computer. In either case, before you use a Management Server or agent-managed computer as a proxy agent, the feature must first be enabled in the Operations console.</p> <p>You must enable the Allow This Server To Act As A Proxy And Discover Managed Objects On Other Computers option on the Security tab of either the Management Server or Agent Managed Computer properties.</p>
Summary	<p>On the Summary page, you can change the agent installation directory. By default, it is set to %ProgramFiles%\System Center Operations Manager.</p> <p>You can also specify the agent action account that you use to run rules and responses on the computer. By default, this is set to Local System. By clicking Other, you can specify the credentials of a domain account to use. This is useful in low-privileged scenarios where local system or local administrative rights might not be appropriate. Instead, you can specify a domain account. This account must have the minimum permissions applied to perform the actions of the relevant Management Packs that will be installed on the managed computer.</p>

During agent installation, an Agent Management Tasks Status window displays the computers on which the agent is being installed. This window includes the installation status, such as Success or Failed. If the agent installation fails, information that relates to the possible cause of the failure is also displayed.

Typical failures include permissions issues where the Management Server action account, or the account that is specified to discover and install the agent, does not have local administrative rights on the

computer. Typical output from this type of failure includes a message that states that the Operations Manager Server could not open service control manager. The following error code is also displayed: 80070005.

After the agent is installed, you can view the agent in either the Administration or Monitoring pane of the Operations console:

- The Agent Managed view under the Device Management node of the Administration pane displays all agent-managed computers. This includes their health state and the primary Management Server to which they are assigned.
- The Window Computers view in the Monitoring pane displays all discovered Windows-based computers. The Agent column displays the health state of the Operations Manager agent that runs on the selected computer.

 **Note:** You can also use the Install-SCOMAgent PowerShell Cmdlet to perform a push-install of an Operations Manager agent. The following commands install an Operations Manager agent on a server named LON-AP2.Contoso.com:

```
$InstallAccount = Get-Credential
$PrimaryMgmtServer = Get-SCOMManagementServer -ComputerName "LON-MS1.Contoso.com"
Install-SCOMAgent -DNSHostName "LON-AP2.Contoso.com" -PrimaryManagementServer
$PrimaryMgmtServer -ActionAccount $InstallAccount
```

Manual Installation

Manual installation of the Operations Manager agent is typically required in the following scenarios:

- Where there is a trust boundary between the Operations Manager Management Group domain and the domain (or workgroup) in which the computer to be managed resides.
- A Gateway Server cannot be used.

The boundary is typically protected by a firewall in which the relevant IP ports that are used when adopting the Push deployment method are not available. In this case, you can install the agent manually in either of the following ways:

- By using setup.exe from the Operations Manager 2012 media.
- By directly running the MOMAgent.msi program that is included with the Operations Manager 2012 media.

You use **MOMAgent.msi** to manually install an agent and specify:

- Management Group name
- Management Server name
- Management Server port
- Agent action account

In this scenario, where the computer to be managed is not located in the same domain as the Management Server domain and no trust is in place, use a certificate to provide mutual authentication between the computer to be managed and the Management Server to which the computer will be assigned. You can install a certificate directly on the managed computer, or deploy a Gateway Server when there are more than five computers to manage. The certificate is installed on the Gateway Server and provides mutual authentication for agents in the managed computer domain.

When you install the agent by using MOMAgent.msi, use the Microsoft Monitoring Agent Setup wizard to collect the required relevant information.

Detailed in the following table are the key pages of the Microsoft Monitoring Agent Setup wizard, including a description of the settings on each page.

Microsoft Monitoring Agent Setup wizard page	Description
Agent Setup Options	<p>By default, the Use Active Directory to configure the agent based on centrally administered settings check box is selected. Use this option to configure the agent to query AD DS for the list of Management Groups to which the agent will report. This option is always enabled when you perform manual installations by using MOMAgent.MSI. This option is covered in more detail in the topic "Active Directory Integration" later in this lesson.</p> <p>The Enable local collection of IntelliTrace logs check box is also selected by default.</p> <p>If the Connect the agent to System Center Operations Manager check box is cleared, the Microsoft Monitoring Agent Setup wizard assumes the agent will be assigned to a Management Group in AD DS. For the purposes of this topic, assume that the Connect the agent to System Center Operations Manager check box is selected.</p>
Management Group Configuration	<p>On the Management Group Configuration page, specify the Management Group Name, Management Server, and Management Server Port. By default, the Management Server Port is 5723. This is the default Agent to Management Server communication port.</p>
Agent Action Account	<p>On this page, you specify either Local System (the default setting) or Domain or Local Computer Account. When you select the Domain or Local Computer Account option, you can specify either the credentials of a domain account or a local computer account. This is useful when the agent is being installed on a computer in a workgroup or in a non-domain-joined computer where a low-privileged account can be used.</p>

You can install the agent from the command prompt by using MOMAgent.msi. The agent can also be scripted. This installation method is typically used by software deployment products, such as Microsoft System Center 2012 R2 Configuration Manager. By using a command-line script, you can use the USE_SETTINGS_FROM_AD switch to configure the agent to obtain its Management Group settings from AD DS.

A typical agent installation command-line script, where the agent obtains its Management Group information from AD DS, is as follows.

```
msiexec /i \\path\Directory\MOMAgent.msi /qn /l*v %temp%\\
mominst.NoGroupSpecified.log USE_SETTINGS_FROM_AD=1 ACTIONS_USE_COMPUTER_ACCOUNT=1
USE_MANUALLY_SPECIFIED_SETTINGS=0 SET_ACTIONS_ACCOUNT=1
```

Be aware that for many organizations, manual installation of the Operations Manager agent is preferred. This provides more control with agent installations in a production environment.

Active Directory Integration

Integrating Operations Manager with AD DS enables agents to automatically obtain their Management Group settings from AD DS. This is especially helpful if your organization uses images or automated build methods to deploy computers.

For example, you can add the Operations Manager agent to the Windows Server 2012 image and configure the agent to obtain its Management Group information from AD DS. When you start a new Windows Server 2012 image, the server is automatically assigned to the appropriate Operations Manager Management Group.

To assign agents to Management Groups by using AD DS, the functional level of the Active Directory domains must be Windows 2000 native or Windows Server 2003 mixed, at a minimum.

To configure Active Directory Integration in Operations Manager, three tasks must be performed, as follows:

1. The MOMADAdmin.exe utility is found in the SupportTools folder on the Operations Manager media. Domain administrators use this utility to create an Active Directory container in the domain in which the Operations Manager Management Group resides. When you use this utility, a security group is specified that is assigned the Read and Delete Child permissions on the container. This then provides Operations Manager administrators with the ability to add Management Servers to the container and to assign computers to the container without being domain administrators.
2. Operation Manager administrators use the Agent Assignment And Failover wizard to assign computers to their primary and secondary Management Servers. When you view the properties of a Management Server in the Management Servers view of the Administration pane, the Add button on the Auto Agent Assignment tab is available in the Agent Assignment And Failover wizard. Described in the following table are the pages of the Agent Assignment And Failover wizard. This includes a description of the settings on each page.

Active Directory Integration gives agents the ability to obtain Management Group information from AD DS.

It is configured by:

1. Using MOMAdmin
2. Using the Agent Assignment And Failover Wizard
3. Installing agents by using **USE_SETTINGS_FROM_AD=1**

Agent Assignment And Failover Wizard page	Description
Domain	You first specify the domain in which the agent-managed computers are located. By default, the current domain is selected. You can manually enter a domain name, or click a trusted domain in the list. To perform the agent assignment, you must also specify an appropriate Operations Manager account. By default, you use Active Directory Based Agent Assignment Account Run As Profile. You can select a different account, or create a new one to perform an agent assignment in the specified domain.
Inclusion Criteria	On this page, you create a LDAP query to use as a filter to match the computer accounts in AD DS that should be included. You can manually enter the LDAP query or click the Configure button to build a query by using fields, such as computer name or owner.
Exclusion Criteria	On this page, you manually enter the FQDN of computers that should be excluded. Multiple computer names are separated by a comma, semicolon, or a new line. For example, this feature is useful when you have specified the Inclusion Criteria that includes

Agent Assignment And Failover Wizard page	Description
	all computers of a particular type, but you know that two of the computers from the list should be excluded because they will be decommissioned. You can manually exclude them by using the Exclusion Criteria.
Agent Failover	On this page, you configure the agent failover. The default setting is Automatically Manage Failover, where agents automatically fail over to other Management Servers in the same Management Group if the primary Management Server is unavailable. You can select the Manually Configure Failover setting where you clear the Management Servers to which you do not want agents to fail over. This setting is useful if there are Management Servers in the Management Group that you know are at their peak for agent management. These Management Servers can be cleared. This means that they will not be used as failover Management Servers.

If additional Management Servers are installed after you run the Agent Assignment And Failover Wizard, you must run the wizard again to have the Management Servers participate in agent assignment and failover.

Be aware that domain controllers should not be included in agent assignment and failover, because they cannot be assigned to a Management Server that uses AD DS. If, when you are running the Agent Assignment and Failover wizard, your Inclusion Criteria includes domain controllers, you should manually add the domain controller FQDN to the Exclusion Criteria.

3. The Operations Manager agent is deployed to the computers by using MOMAgent.msi, and is configured to obtain its Management Group information from AD DS.

For more information about integrating Operations Manager with Active Directory visit the following website.

Integrating Active Directory and Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=404083>

Question: You have manually installed an Operations Manager agent on a computer and specified the correct Management Group settings during the installation. However, the agent is not displayed in the Operations console. What should you do?

Demonstration: Deploying an Operations Manager Agent

In this demonstration you will learn how to deploy an Operations Manager agent using the Operations Console.

Demonstration Steps

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
Link	Discovery Wizard

2. Use the Computer and Device Management wizard to deploy an agent to LON-DC1 with the following settings (leave all other default settings):
 - a. Browse For, Or Type In Computer Names: **LON-DC1**
 - b. Administrator Account: Use the **Other user account** option and enter the credentials for the **Contoso\Administrator** account
 - c. Select Objects To Manage: **LON-DC1.CONTOSO.COM**
 - d. Management Server: **LON-MS1.CONTOSO.COM**.
3. Cancel the wizard without deploying the agent.

Lesson 6

Configuring Agentless Exception Monitoring (AEM)

In organizations where many servers host several different applications, it is sometimes difficult to manage application-related exception errors that occur. Frequently, the IT Administrator is not aware of many application exception errors or crashes that occur on these servers, because this information is not forwarded to Microsoft through error reporting nor to a central share for analysis.

For example, suppose that an application update is applied to 1,000 servers. The update causes the application to stop responding for approximately 30 seconds. This issue is caused by a bug that is resolving the IP address of the database server to which the application connects. An application error is generated in this scenario which is typically stored locally on the server, which is not notified of the generated error.

To capture and analyze events such as these, you must understand how AEM in Operations Manager is configured.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe AEM.
- Enable AEM.
- Configure a server for AEM.

Overview of Agentless Exception Monitoring (AEM)

AEM is part of the Client Monitoring feature in Operations Manager. It collects and centrally stores information about operating system and application errors. It also provides views and reports that contain details about the computers and users who are affected by errors, including the frequency of the errors in the environment.

By default, a report is generated when a Microsoft application experiences an error or an exception occurs. The report contains details of the error, including the computer that was affected, the application name, and the user who was logged into the system at the time.

If the computer is configured appropriately, this information is sent to Microsoft as part of the Customer Experience Improvement Program (CEIP). Microsoft uses this anonymous information to reduce errors in applications and improve the customer experience.

With AEM, you can collect this data by using a Management Server that is configured for Client Monitoring. The data is then stored on a network share for analysis.

Several views in the Monitoring pane of the Operations console provide analysis of collected data that relate to operating system and application errors. A description of each view is discussed in the following list:

- **Application view.** This is a state view that lists the applications that have experienced a failure.

AEM monitors exceptions by using:

- Application view
- Crash Listener view
- Error Events view
- Error Group view
- System Error Group view
- AEM reports

- **Crash Listener view.** This is a state view that lists the computers that are listening for failures on other computers or applications.
- **Error Events view.** The Error Events view details the application error reports that are generated by applications or operating systems.
- **Error Group view.** This is a state view that displays application errors by error group.
- **System Error Group view.** This is a state view that displays the computers that are experiencing operating system failures.

In addition to the Application Exception Monitoring views in the Monitoring pane, you can use several other reports to help with analyzing application and operating system errors. You can find these reports in the Reporting pane of the Operations console in the Client Monitoring Views Library folder. Listed here are descriptions of the available reports:

- **Top N Applications.** This report provides a chart that displays the top N applications that are based on crash count. Included with the report is a table that lists the application name, serial number, version, crash count, and average daily crash count.
- **Top N Applications Growth and Resolution.** Based on the selected time interval, a chart displays the top N applications that are based on their growth percentile. Included with the report is a table that details the top N applications based on their crash count. The table also includes details of the crash count growth percentile from the first time interval and the latest time interval.
- **Top N Error Groups.** This report displays a chart that displays the top N error groups based on crash count. A table is also included that displays the total crash count, average crash count per error group, and the average daily crash count per error group.
- **Top N Error Groups and Resolution.** Based on the selected time interval, a chart displays the top N error groups based on their growth percentile. Included with the report is a table that details the top N error groups based on their crash count. The table also includes details of the crash count growth percentile from the first time interval and the latest time interval.

Using a combination of views and reports, you can perform a detailed analysis of application and operating system exception errors.

In addition to collecting and combining error reports, AEM can also forward the collected data to Microsoft and participate in CEIP. This also provides links to solutions for the errors that are reported.

The Process of Configuring the Management Server for AEM

Configuring AEM in Operations Manager is a two-step process. First, you run the Client Monitoring Configuration Wizard. This is located on a Management Server through the Management Servers view in the Device Management node of the Operations console in the Administration pane. Then, a Group Policy Administrative Template that was created when you ran the Client Monitoring Configuration Wizard is applied and configured on either the domain or the local computer policy.

The following table describes the Client Monitoring Configuration Wizard.

The Client Monitoring Configuration wizard configures:

- CEIP forwarding
- Error collection
- Error forwarding
- File share
- Client settings

Client Monitoring Configuration Wizard page	Description
CEIP Forwarding	<p>On this page, you configure the CEIP settings. By default, CEIP data is sent directly to Microsoft, or you can use the selected Management Server to collect and then forward CEIP data to Microsoft. When you select the latter option, you can also enable SSL (the default is enabled) and whether Windows Authentication should be used. If SSL is required, the SSL certificate must be installed on the Management Server.</p>
Error Collection	<p>On this page, you specify the error collection settings, such as the following:</p> <ul style="list-style-type: none"> • The file share path. • Whether SSL should be used. • Whether error reports should be collected from operating system clients running Windows Vista or newer versions. • The organization name. This is particularly useful especially when errors are displayed in pop-ups windows. <p>A file share with the necessary permissions is created automatically.</p>
Error Forwarding	<p>On this page, you select whether collected errors should be forwarded to Microsoft. By default, collected errors are not forwarded. When you select this option, you can also decide to send either basic (the error signature) or detailed (the error signature and requested additional data) error reports.</p>
Create File Share	<p>On this page, you specify the credentials to use to create the file share where collected error reports will be stored. You can select either an existing action account, or manually add the credentials of an account that has the required permission to create the share. For example, an Existing action account is useful when you do not want the operator to know the password, such as in a high-security environment.</p>
Task Status	<p>On this page, a task is run to create the file share on the selected Management Server. If there are any problems running the task, errors are displayed on this page.</p>
Client Settings	<p>On this page, you specify the location where the Group Policy administrative template should be saved. This location is used to configure the domain or local computer policy settings for AEM.</p>

Common Policy Settings for Configuring Servers for AEM

When the Client Monitoring Configuration Wizard has completed a Group Policy, an administrative template is generated. Use this template to configure the domain or local computer policy. Add the template to the Computer Configuration\Administrative Templates policy by using the Add\Remove task in the Local Group Policy Editor for the local computer or domain.

The template adds several policy settings to configure client monitoring on computers in the domain. For settings to be effective, you must disable the Turn off Windows Error Reporting policy. By disabling this policy, error reports are forwarded to a file share. You can find the policy in Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings in the Local Group Policy Editor.

Described in the following table are some common policy settings that you can configure after you apply the AEM administrative template.

- AEM Administrative Template includes policies for:**
- CEIP
 - Error notification
 - Error reporting
 - Operating system errors
 - Application errors

AEM Administrative Template policy name	Description
Configure CEIP (Customer Experience Improvement Program)	This policy should be enabled to allow for CEIP reports to be forwarded to the Management Server. The URL of the Management Server is automatically added to the CEIP settings so that computers know where reports should be sent.
Configure Error Notification	This policy enables error notification and is useful in troubleshooting AEM. You can enable or disable the ShowUI and DoNotDebugErrors options, depending on whether the monitored computers have interactive users.
Configure Error Reporting for Windows Vista And Later Version Operating Systems	This policy enables you to send error reports to the Management Server. When it is enabled, the Error_Listener is populated automatically with the Management Server computer name. Optional settings, such as the Error_ListenerPort, can be configured. Changing the Error_ListenerPort is useful when the port is already being used by another application.
Report Operating System Errors	When error reporting is enabled, this policy lets operating system errors be captured.
Application Reporting Settings (All Or None)	When error reporting is enabled, this policy lets application errors be captured.

To configure the AEM policy settings, after you apply the administrative template, open the local or Domain Group Policy Management Console, and then browse to Computer Configuration\Administrative Templates\Classic Administrative Template (ADM)\Microsoft Applications\System Center Operations Manager (SCOM). From here you can configure relevant policy.

Question: When you configure AEM in your environment, what Group Policy must be disabled before the AEM administrative template is applied?

Lesson 7

Configuring Audit Collection Services

ACS in Operations Manager has the ability to collect security events that are based on your security auditing requirements. In many organizations, security event logs must be kept for long periods of time. This allows for audits to be performed when a security breach is detected. One industry in which security event logs might be kept for a long period of time is the payment card industry.

Organizations who store sensitive data such as credit card details must keep records of security events for many years. These organizations must be able to prove that the data is being stored securely.

Operations Manager not only lets you collect and store security event logs, it also includes several built-in reports that you can use to provide analysis of many security-related scenarios, such as account logon failures and object permission changes.

You must understand the components on which ACS relies, and how you can configure these components to collect security event data in your environment.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe the components of ACS.
- Describe how to install ACS.
- Describe how to filter the data that ACS collects.
- Describe how to configure reporting for ACS.

Audit Collection Services (ACS) Architecture

There are three components that ACS requires to collect and store security event log data. These are the ACS Forwarders, ACS Collector, and ACS Database. Each component is described here, including how they integrate with one another.

ACS Forwarders

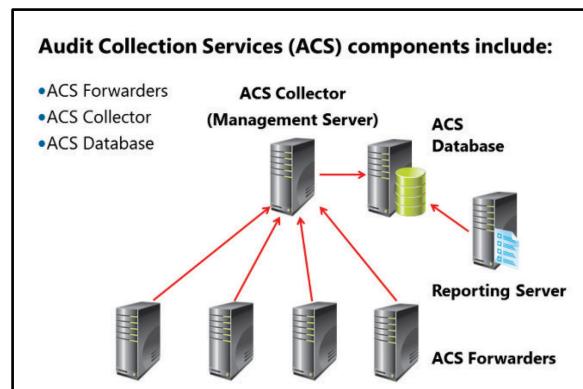
When an Operations Manager agent is installed on a computer that is to be managed, an additional service named System Center Audit Forwarding is also installed. By default, this service is disabled.

You can enable this service by running the Enable Audit Collection task from the Operations console.

You can use this task to enable audit collection on multiple computers at the same time. This saves time when there are several computers from which you must collect security events, such as all domain controllers. When the service is running, it collects all security events from the security event log and sends them to the ACS Collector.

ACS Collector

The ACS Collector component is installed on an Operations Manager Management Server. It collects security event data from ACS Forwarders, processes it, and then stores the data in the ACS Database. During the processing of the security event data, you can apply a filter to reduce the volume of data that



is stored in the ACS Database. Additionally, the data is spread across multiple tables within the database. This minimizes data redundancy and improves performance when you are running ACS reports.

Be aware that there is a limit to the number of ACS Forwarders that an ACS Collector and an ACS Database can support. This is determined by several factors, including the following:

- **Audit Policy.** Depending on your audit policy, the number of security events that are generated will differ greatly. For example, you might have to audit object access to sensitive files and audit both the successful and failed account logons. This generates much more event data than just auditing account logon failures.
- **Computer Role.** The amount of security event data that is generated depends on the role of the monitored computer on which the ACS Forwarder is installed. For example, a domain controller typically generates more security-related events than a member server.
- **Computer Activity.** Related to the computer role is the activity that is performed on the computers on which the ACS Forwarders are running. For example, a computer that hosts the database that stores payment card details will typically be more active than a computer that hosts a payroll application that is run only one time per month.
- **Hardware.** The hardware on which the ACS Collector and ACS Database are hosted is also an important factor when collecting and storing security event data.

You can deploy multiple ACS Collectors when there are too many ACS Forwarders for one ACS Collector to manage. However, each ACS Collector must have its own dedicated ACS Database. The minimum hardware and software requirements for an ACS Collector are noted here:

- Must be an Operations Manager Management Server
- A minimum of 1 gigabyte (GB) of RAM (2 GB is recommended)
- A minimum of 1.8-gigahertz (GHz) processor (2.8 GHz is recommended)
- A minimum of 10 GB of available disk space (50 GB is recommended)

ACS Database

The ACS Database stores the security event data that is collected by the ACS Collectors. Although the database can be installed on the same computer as the ACS Collector, it is recommended that you store the database on a dedicated computer for performance and scalability reasons. The minimum hardware and software requirements for the ACS Database are as follows:

- SQL Server 2008 R2 Service Pack 1 (SP1), SQL Server 2008 R2 Service Pack 2 (SP2), SQL Server 2012, or SQL Server 2012 SP1
- A minimum of 1 GB of RAM (2 GB is recommended)
- A minimum of 1.8-Ghz processor (2.8 Ghz is recommended)
- A minimum of 20 GB of available disk space (100 GB is recommended)

SQL Server Enterprise edition is recommended for the ACS Database. With SQL Server Standard edition, the ACS Database is paused during daily maintenance operations. This can cause the ACS Collector queue to become full and cause a disconnected ACS Forwarder. When this happens, the ACS Forwarder stores collected data locally until it can reconnect to its ACS Collector. Therefore, it is recommended that you size the security event log appropriately on the computer that is hosting the ACS Forwarder. Security event data can be lost if the ACS Forwarder loses connection to its ACS Collector, and there is insufficient space allocated to the security event log.

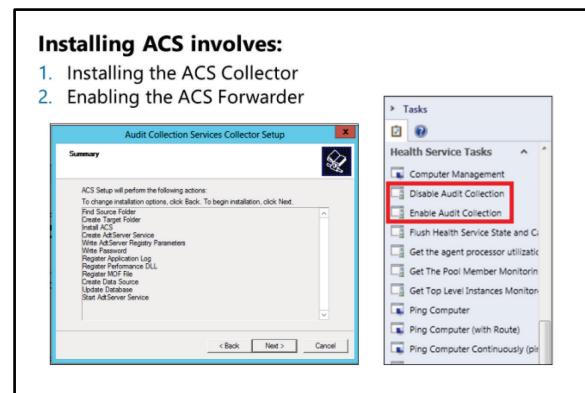
With SQL Server Enterprise edition, this condition does not occur, because the ACS Database is not paused during daily operations.

ACS Security

By default, data is encrypted between the ACS Forwarder and the ACS Collector when both are in the same or trusted domain. By default, data between the ACS Collector and the ACS Database is not encrypted. For organizations that require encrypted data between the ACS Collector and the ACS Database, SSL certificates can be used. To make this easier, SSL certificates are installed on both the ACS Collector and the ACS Database server.

Install ACS

ACS is installed by clicking the Audit collection services link in the Optional Installation section of the Operations Manager installation screen. When you run an ACS installation, the Audit Collection Collector Setup Wizard guides you through the setup options, as described in the following table.



Audit Collection Services Collector Setup Wizard page	Description
Database Installation Options	On this page, you select either to create a new ACS Database (the default setting) or to use an existing ACS Database. When setup creates a new database, it automatically creates the necessary logon and database user for the ACS Collector. Typically, you use only an existing database when you are reinstalling an ACS Collector. Additionally, you can manually create the database by using a set of SQL scripts that are provided in the ACS folder on the Operations Manager media. Typically, you manually install the ACS Database when the database server is behind a firewall that restricts the ACS setup from accessing it.
Data Source	For the ACS Collector to communicate with the SQL Server that hosts the ACS Database, an Open Database Connectivity (ODBC) Data Source is created. This page is where you can change the data source name (DSN). By default, the DSN is set to OpsMgrAC.
Database	On this page, you add the SQL Server computer name and database server instance in which the ACS Database will be created. You can also change the database name. The default database name is OperationsManagerAC. Additionally, if you are running setup on the SQL Server itself, you can click the Database Server Running Locally option.
Database Authentication	On this page, you specify the authentication that should be used when you connect to the SQL Server. By default, Windows authentication is selected. In this case, the ACS Collector's computer account will be used to authenticate to the SQL database. Or, you can select SQL Authentication. This is typically used when the ACS Collector and SQL Server are not in the same domain or in a trusted domain. When you use SQL authentication, the user System Administrator cannot be used.

Audit Collection Services Collector Setup Wizard page	Description
Database Creation Options	On this page, you select where the database files will be located. By default, every database has at least two files: the database file and the log file. As a best practice, it is recommended that you store these files on different physical hard disks, and on different physical hard disks from the page file and operating system. You can select the location of the database and log file, or use the SQL Server's default data and log file directories.
Event Retention Schedule	On this page, you specify the number of days that events should be retained in the ACS Database. By default, this is 14 days. You also specify the hour of the day in which the daily database maintenance should be performed. This is important, because database performance is affected during database maintenance. Therefore, you should specify a time of day that is not especially busy, for example, early morning or late evening. The default hour is 2:00 A.M.
ACS Stored Timestamp Format	On this page, you specify the time stamp that is applied to the ACS Database. By default, time stamps in the database are adjusted to the local time on the database server. Or, you can select Universal Coordinated Time (UTC). This is typically used where precision time stamps are required. It is also used by many Internet and World Wide Web (WWW) standards.

Enabling Audit Collection on the ACS Forwarders

Before security event data can be forwarded to ACS Collectors, the ACS Forwarders must be enabled on the computers that are hosting the Operations Manager agent and the System Center Audit Forwarding service.

This is performed by using the Enable Audit Collection task in the Operations console. The task becomes available by using several views in the Monitoring pane. By selecting the Agents By Version view from the Agent Details subfolder of the Operations Manager folder, the Details pane lists the computers that have an Operations Manager agent installed. When you select one or more computers, the Enable Audit Collection task becomes available in the Tasks pane under Health Service Tasks.

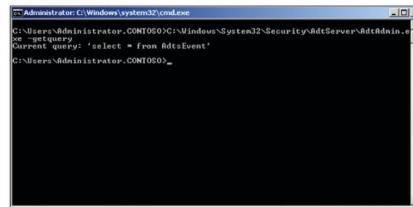
When you run the task, use an override to specify the ACS Collector that will be associated with the ACS Forwarders and to which the ACS Forwarders should send event data. When the task has completed, the task output displays the Agent Management Group name and the result from starting the System Center Audit Forwarding service. Use this information to troubleshoot failed tasks where the account that is used to run the task might not have sufficient permissions.

At this point, the System Center Audit Forwarding service is started on the selected computers, and its startup type is set to Automatic.

Filter Data Collected by ACS

Before you implement ACS, you should make sure that your audit policy was applied to all the Operations Manager agent-managed computers from which you must collect security event data. Your audit policy determines which events should be written to the security event log. These events include all other security events that are written to the security event log that is sent to the ACS Collector. This can result in a large volume of data being sent to the ACS Collector. The ACS Collector then processes the events and inserts them into the ACS Database.

The **AdtAdmin** utility is used to create a filter used by ACS



To reduce the volume of sent data and to eliminate noise events, you configure a filter on the ACS Collector. The filter is formatted as WMI Query Language (WQL).

The applied default filter collects all security events that are written to the security event log and is denoted as follows: **select * from AdtsEvent**. The filter is controlled through the AdtAdmin command-line utility.

The AdtAdmin utility is located in the C:\Windows\System32\Security\AdtServer folder and has 12 parameters. Only two of these parameters are relevant in setting the collector site filter, as described in the following table.

Parameter	Description
-getquery	Displays the WQL queries that are active on an ACS Collector
-setquery	Configures the WQL query that the ACS Collector uses to filter audit event data

For a complete listing of the **AdtAdmin** parameters, run the **AdtAdmin** command with the **/?** switch.

For more information on the AdtAdmin tool, visit this webpage.

ACS Administration--AdtAdmin.exe

<http://go.microsoft.com/fwlink/?LinkId=391265>

How to Set the Filter

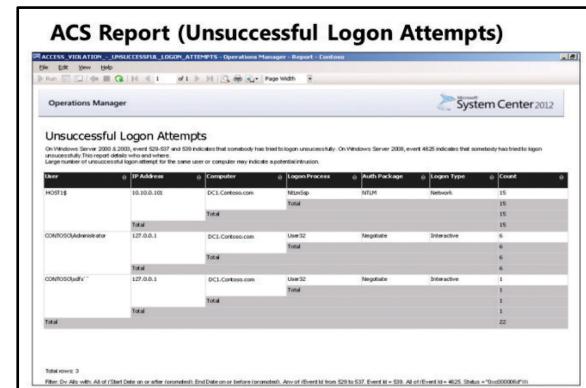
Use the **AdtAdmin -setquery** command to set the query for the filter. This command has two subparameters: **-collector**, and **-query**. Use the **-collector** parameter to specify to which collector to connect. The **-query** parameter specifies the syntax of the query.

In the following example, the **-setquery** command is used to filter events that are logged by SYSTEM, LOCAL SERVICE, and NETWORK SERVICE. Additionally, Event IDs 538, 566, 672, 680, 541, and 547 will also be filtered out.

```
AdtAdmin /setquery -collector "Collector Name" -query "SELECT * FROM AdtsEvent WHERE NOT ((HeaderUser='SYSTEM' OR HeaderUser='LOCAL SERVICE' OR HeaderUser='NETWORK SERVICE') OR (EventId=538 OR EventId=566 OR EventId=672 OR EventId=680) OR (EventId>=541 AND EventId<=547))"
```

The Process of Configuring Reporting for ACS

By default, there are no reports available in Operations Manager for ACS. Before you can use ACS reports in Operations Manager, you must import them into the SQL Server Reporting Services Server. The following table describes the steps that must be followed when enabling ACS reports in Operations Manager.



Enabling ACS Reporting step	Description
Copy the ACS folder from the Operations Manager media.	In the ReportModels folder on the Operations Manager media, copy the ACS folder and its contents to a computer that has access to the SQL Server Reporting Services Server.
At a command prompt, run UploadAuditReports .	<p>Open a command prompt window on the computer that contains the ACS folder, and then browse to the ACS folder. Run the following command.</p> <pre>UploadAuditReports <databaseserver\instance> <ReportingServiceURL> <ReportFolder></pre> <p>The following is an example.</p> <pre>UploadAuditReports LON-SQ1 http://LON-SQ1/ReportServer C:\ACS</pre>
Configure the data source.	Open the SQL Server Reporting Services Server Web console at <a href="http://<ReportingServiceServer>/Reports">http://<ReportingServiceServer>/Reports . Open the DB Audit data source from the Audit Reports folder. Make sure that the Windows Integrated security is selected, and then click Apply.

The ACS reports are now available from the Reporting pane of the Operations console in the Audit Reports folder.

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
The ACS Collector runs on an agent-managed computer and forwards security event data to the ACS database. Is this true or false?	

Question: On which server should the ACS Collector be installed?

Lab: Installing System Center 2012 R2 Operations Manager and Deploying Agents

Scenario

You have been tasked with installing and configuring a new Operations Manager environment for Contoso, Ltd. The environment includes three domain-joined Windows Server 2012 R2 computers that will be used to host the Operations Manager components. The computer named LON-SQ1 has already been configured with SQL Server 2012 and will be used to host the Operations Manager databases. Computers LON-MS1 and LON-MS2 will be used as Management Servers for the new Operations Manager Management Group.

There is also a requirement to monitor a number of computers in an untrusted environment, which the Contoso, Ltd. domain does not have access to. To facilitate this, you must install and configure a Gateway Server in the untrusted domain.

After deploying the Management Group, you must install the Operations Manager Agent and configure AD DS integration to monitor the Contoso environment.

As part of Contoso's security mandate, all logon failures must be recorded and tracked for auditing. In addition, a report must be available that describes the computers and accounts that were used to access them. To make this recording and tracking easier, you must configure Audit Collection Services in Operations Manager.

Following a business-critical application update, many users are experiencing Dr. Watson errors when they start the application. You decide to configure Agentless Exception Monitoring. This lets you analyze the number of application exceptions and determine the scope of the problem.

Objectives

After completing this lab, you will be able to:

- Install a new System Center 2012 R2 Operations Manager Management Group.
- Install and configure a System Center 2012 R2 Operations Manager Gateway Server.
- Install Operations Manager Agents.

Lab Setup

Estimated Time: 60 minutes

Virtual Machines: 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-MS2, 10964C-LON-GW1, 10964C-LON-AP2, 10964C-LON-AP1

User Name: Contoso\Administrator

Password: Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**

- Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:
- 10964C-LON-SQ1
 - 10964C-LON-MS1
 - 10964C-LON-MS2
 - 10964C-LON-GW1 (Logon using the local Administrator with a password of Pa\$\$w0rd)
 - 10964C-LON-AP2
 - 10964C-LON-AP1



Note: The following exercises in this Lab are optional:

- Installing and Configuring the Gateway Server.
- Installing and Configuring Audit Collection Services (ACS).
- Configuring Agentless Exception Monitoring (AEM).

Exercise 1: Installing a New System Center 2012 R2 Operations Manager Management Group

Scenario

One main difference between Operations Manager 2007 and Operations Manager 2012 is that the root management server (RMS) is no longer used. With Operations Manager 2012, all Management Servers are considered peers. This topology change immediately removes the single point of failure that is present in Operations Manager 2007. In this exercise, you deploy a new Operations Manager 2012 R2 Management Group.

The main tasks for this exercise are as follows:

1. Install the first Management Server
2. Install the second Management Server
3. Install the Reporting server
4. Install the Web console server

► Task 1: Install the first Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Manager Setup
Location	\LON-DC1\Media \LON-DC1\Media\SCOM2012R2
Setup file	ReportViewer.msi Setup.exe

2. Install Report Viewer from **\LON-DC1\Media** using default settings.
3. Install Operations Manager by using **Setup.exe** from **\LON-DC1\Media\SCOM2012R2** with the following settings (all other settings should be left as the default):
 - a. Features to install: **Management Server** and **Operations Console**
 - b. Management Group Name: **SCOM2012**
 - c. Server name and instance name: **LON-SQ1**



Note: **LON-SQ1** should be used as the **Server name and instance name** for both the operational database and data warehouse database.

- d. Configure Operations Manager accounts:

Account Name	Domain\User Name	Password
Management Server action account	Contoso\svc_SCOM2012_msaa	Pa\$\$w0rd
System Center Configuration service and System Center Data Access service	Contoso\svc_SCOM2012_das	Pa\$\$w0rd
Data Reader account	Contoso\svc_SCOM2012_dwread	Pa\$\$w0rd
Data Writer account	Contoso\svc_SCOM2012_dwwrite	Pa\$\$w0rd

► Task 2: Install the second Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Operations Manager Setup
Location	\LON-DC1\Media \LON-DC1\Media\SCOM2012R2
Setup file	ReportViewer.msi Setup.exe

2. Install ReportViewer by using the default settings.
3. Install Operations Manager by using the following settings (all other settings should remain as the default):
- Features to install: **Management Server** and **Operations Console**
 - Specify an Installation option: **Add a Management server to an existing management group**
 - Server name and instance name: **LON-SQ1**
 - Database: **OperationsManager**
4. Configure Operations Manager accounts:

Account Name	Domain\User Name	Password
Management Server action account	Contoso\svc_SCOM2012_msaa	Pa\$\$w0rd
System Center Configuration service and System Center Data Access service	Contoso\svc_SCOM2012_das	Pa\$\$w0rd

► Task 3: Install the Reporting server

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-SQ1
Tool	Internet Explorer
URL	http://LON-SQ1/Reports

- Confirm the **SQL Server Reporting Services Home** page loads in **Internet Explorer** then close **Internet Explorer**.
- Run **setup.exe** from **\LON-DC1\Media\SCOM2012R2**.
- Install Operations Manager by using the following settings (all other settings should remain as the default):
 - Features to install: **Reporting server**
 - Management server name: **LON-MS1**
 - Configure Operations Manager accounts: **Contoso\svc_SCOM2012_dwread** and **Pa\$\$w0rd**
- Open the Operations console on **LON-MS1**, and then confirm the **Reporting** pane is available.

► Task 4: Install the Web console server

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Manager Setup
Location	\LON-DC1\Media\SCOM2012R2
Setup file	Setup.exe

- Add the Web console feature by using the following settings (all other settings should remain as the default):
 - Features to install: **Web Console**
 - Confirm that **read** and **write** permissions on the: **C:\Windows\Temp** folder for **LON-MS1\IIS_IUSRS** and **NETWORK SERVICE** have been set.
- Browse to **http://LON-MS1/OperationsManager**, and then confirm the Web console opens.



Note: If a **Web Console Configuration Required** webpage appears use the **Configure** button to configure **Silverlight** and then if the **Web Console Configuration Required** webpage reappears click **Skip**.

Results:

After this exercise, you should have performed a new installation of Microsoft System Center 2012 R2 Operations Manager. This includes two Management Servers: the Reporting Server and the Web console.

Exercise 2: Installing and Configuring the Gateway Server

Scenario

A number of computers in an untrusted domain need to be monitored, so you must install and configure a Gateway Server. The Gateway Server will communicate with the agents in the untrusted domain and then (by using certificates) will pass monitored data to a Management Server in the domain where the Operations Manager Management Group resides.

The main tasks for this exercise are as follows:

1. Import the root CA certificate chain on the Gateway Server
2. Import the root CA certificate chain on the Management Server
3. Request the Gateway Server certificate
4. Issue the Gateway Server certificate
5. Import the Gateway Server certificate
6. Request the Management Server certificate
7. Issue the Management Server certificate
8. Import the Management Server certificate
9. Import the Management Server certificate into Operations Manager and approve the Gateway Server
10. Install the Gateway Server
11. Import the Gateway Server certificate into Operations Manager
12. Confirm the Gateway Server is communicating with the Management Server

► Task 1: Import the root CA certificate chain on the Gateway Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-GW1
Tool	Internet Explorer
URL	https://LON-AP2/certsrv
Link	Download a CA certificate, certificate chain or CRL

2. Download the CA certificate chain to the desktop, and then follow these steps:

- a. Open Microsoft Management Console (MMC), and then add the Certificates snap-in for the local computer.
- b. Import the certificate into the Trusted Root Certification Authorities store.

► **Task 2: Import the root CA certificate chain on the Management Server**

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Internet Explorer
URL	https://LON-AP2/certsrv
Link	Download a CA certificate, certificate chain or CRL

- Download the CA certificate chain to the desktop, and then follow these steps:

- Open MMC, and then add the Certificates Snap-in for the local computer.
- Import the certificate into the Trusted Root Certification Authorities store.

► **Task 3: Request the Gateway Server certificate**

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-GW1
Tool	Internet Explorer
URL	https://LON-AP2/certsrv
Link	Request a certificate

- Use the **Request a certificate\Advanced certificate request** link to request a certificate for the Gateway Server by using the following settings (all other settings should remain as the default):

- Type of certificate needed: **Other**
- OID: **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2**



Note: Notice that a comma (,) is used in the middle of the OID value.

- Name: **LON-GW1**
- Friendly name: **LON-GW1**
- Mark keys as exportable: **Yes**
- Submit the request
- Leave Internet Explorer open.



Note: The OID (Object ID) value is used to identify the purpose of which the certificate is valid for. The 1.3.6.1.5.5.7.3.1 OID value represents a server certificate whereas the 1.3.6.1.5.5.7.3.2 OID value represents a client certificate.

► **Task 4: Issue the Gateway Server certificate**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-AP2
Tool	Certification Authority
Location	Administrative Tools
View	Pending Requests

2. Right-click the pending request, and then click **Issue** to issue the request.

► **Task 5: Import the Gateway Server certificate**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-GW1
Tool	Internet Explorer
URL	https://LON-AP2/certsrv
Link	View the status of a pending certificate request

2. Install the certificate, and then import the certificate by using the following procedure:

- a. Open MMC, and then add the **Certificates** snap-in for **Computer account** and **My user account**.
 - b. Expand the current user certificates, and from the **Personal** folder, export the certificate to the desktop, and then name the file **LON-GW1**.
 - c. Use the password **Pa\$\$w0rd**.
3. Expand the local computer certificates, and from the **Personal** folder, import the **LON-GW1** certificate.

► **Task 6: Request the Management Server certificate**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Internet Explorer
URL	https://LON-AP2/certsrv
Link	Request a certificate

2. Use the **Request a certificate\Advanced certificate request** link to request a certificate for the Gateway Server by using the following settings (all other settings should remain as the default):
 - Type of certificate needed: **Other**
 - OID: **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2**
 - Name: **LON-ms2.contoso.com**
 - Friendly name: **LON-ms2.contoso.com**
 - Mark keys as exportable: **Yes**
3. Submit the request.

► **Task 7: Issue the Management Server certificate**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-AP2
Tool	Certification Authority
Location	Administrative Tools
View	Pending Requests

2. Right-click the pending request, and then click **Issue** to issue the request.

► **Task 8: Import the Management Server certificate**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Internet Explorer
URL	https://LON-AP2/certsrv
Link	View the status of a pending certificate request

2. Install the certificate, and then import the certificate by using the following procedure:

- a. Open MMC, and then add the **Certificates** snap-in for **Computer account** and **My user account**.
 - b. Expand the current user certificates, and from the **Personal** folder, export the certificate to the desktop, and then name the file **LON-MS2**.
 - c. Use a password of **Pa\$\$w0rd**.
3. Expand the local computer certificates, and from the **Personal** folder, import the **LON-MS2** certificate.

► **Task 9: Import the Management Server certificate into Operations Manager and approve the Gateway Server**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	MOMCertImport.exe
Location	\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64
Certificate	LON-MS2

2. Import the LON-MS2 certificate by using the **MOMCertImport** tool from the location specified above.

3. Approve the Gateway server by performing the following steps:

- a. From **\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64**, copy **Microsoft.EnterpriseManagement.GatewayApprovalTool** to **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server**.
- b. Open a Command Prompt window, and then browse to **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server**.
- c. At the command prompt, type the following, and then press Enter.

```
Microsoft.EnterpriseManagement.GatewayApprovalTool.exe /ManagementServerName=LON-MS2.CONTOSO.COM /GatewayName=LON-GW1 /SiteName=London /Action/Create
```

► Task 10: Install the Gateway Server

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-GW1
Tool	MOMGateway.MSI
Location	C:\Gateway\AMD64
Application	MOMGateway

- Run **MOMGateway** to install the Gateway Server that has the following settings (all other settings should remain as the default):
 - Management Group Name: **SCOM2012**
 - Management Server: **LON-MS2.contoso.com**
- User Account: **Local System**

 **Note:** During the installation of the **Gateway Server** a message stating “**Setup failed to enumerate trusted domains**” will appear. This is expected and can be ignored.

► Task 11: Import the Gateway Server certificate into Operations Manager

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-GW1
Tool	MOMCertImport.exe
Location	\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64
Certificate	LON-GW1

- Run **MOMCertImport**, and import the LON-GW1 certificate.

► **Task 12: Confirm the Gateway Server is communicating with the Management Server**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Operations Console
Pane	Administration
View	Device Management\Management Servers

2. Refresh the view, and then confirm **LON-GW1** is displayed and is healthy.



Note: It can take up to 5 minutes for the **LON-GW1** server to appear.

Results: After this exercise, you should have installed and configured an Operations Manager Gateway Server on LON-GW1. This involves importing the root certificate chain on both the Gateway Server, and the Management Server that will manage the Gateway Server. Then, you would have requested, issued, and imported a server certificate for both the Management Server and the Gateway Server. Finally, you will have installed the Gateway Server on LON-GW1, and then used the MOMCertImport tool to import the Gateway Server certificate into Operations Manager.

Exercise 3: Installing the Operations Manager Agent

Scenario

Before monitoring business-critical computers and applications, you must deploy an Operations Manager agent on them. In this scenario, where the computers are in a mutually trusted environment, you can use the Operations console to push-install the agent. Where computers are in a perimeter network environment in which remote procedure call (RPC) access to the agent from the Operations console is restricted, you will need to install the Operations Manager agent manually.

The main tasks for this exercise are as follows:

1. Perform a push-install of the Operations Manager agent
2. Allow manual agent installations in Operations Manager
3. Install the Operations Manager agent manually
4. Use the Operations console to approve a manually installed agent

► Task 1: Perform a push-install of the Operations Manager agent

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
Link	Discovery Wizard

2. Use the Computer and Device Management wizard to deploy an agent to LON-DC1 and LON-SQ1 with the following settings (leave all other default settings):
 - a. Browse For, Or Type In Computer Names: **LON-DC1, LON-SQ1**
 - b. Administrator Account: Use the **Other user account** option and enter the credentials for the **Contoso\Administrator** account
 - c. Select Objects To Manage: **LON-DC1.CONTOSO.COM** and **LON-SQ1.CONTOSO.COM**
 - d. Management Server: **LON-MS1.CONTOSO.COM**.
3. Confirm that the **LON-SQ1.contoso.com** and **LON-DC1.contoso.com** computers are now displayed in the **Agent Managed** view of the **Device Management** folder in the **Administration** node of the **Administration** pane.

 **Note:** The computers first display a Health State of not monitored. This changes to Healthy after approximately two minutes.

► **Task 2: Allow manual agent installations in Operations Manager**

- To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration\Settings
View	Security

- Edit the **Global Management Server Settings**, and then enable the **Review new manual agent installations in pending management view** setting.

► **Task 3: Install the Operations Manager agent manually**

- To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-AP2
Tool	MOMAgent.msi
Location	\LON-DC1\Media\SCOM2012R2\Agent\AMD64

- Use MOMAgent.msi to install the agent on LON-AP2 with the following settings (leave all other default settings):
 - Management Group Name: **SCOM2012**
 - Management Server: **LON-MS1**

► **Task 4: Use the Operations console to approve a manually installed agent**

- To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration\Device Management
View	Pending Management

- Use **Approve from the Tasks** pane to approve LON-AP2.

Results: After this exercise, you should have installed an Operations Manager agent using the Operations console. You should have also configured Operations Manager to review new manual agent installations and then manually installed and approved an Operations Manager Agent.

Exercise 4: Configuring Active Directory Integration

Scenario

Contoso uses a standard image of the Windows Server 2012 operating system when deploying new servers. This build includes an Operations Manager Agent. For the agent to be automatically assigned to Management Servers in the Management Group, you must configure integration between Operations Manager and AD DS.

The main tasks for this exercise are as follows:

1. Use Momadadmin.exe to configure the Active Directory container
2. Configure the Active Directory Based Agent Assignment Account Run As Profile
3. Use the Agent Assignment and Failover Wizard
4. Install the agent using Momagent.msi
5. Confirm the agent is automatically assigned

► Task 1: Use Momadadmin.exe to configure the Active Directory container

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Command Prompt
Folder	C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server
Command	MomAdAdmin.exe SCOM2012 Contoso\SCOM2012_Admins Contoso\Administrator Contoso

2. On LON-MS1, from a Command Prompt, enter the command listed in the preceding table in the Command Prompt window, and then close the Command Prompt window.

► Task 2: Configure the Active Directory Based Agent Assignment Account Run As Profile

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Run As Configuration\Profiles

2. Configure the **Active Directory Based Agent Assignment Account** as follows, (all other settings should be remain as the default):
 - a. Add a new **Run As Account** with a name of **Administrator** and use the **Contoso\Administrator** credentials.

- b. Use the **A selected class, group or object** option, and add the **AD Assignment Resource Pool** group.
- c. Edit the **Administrator** Run As Account and add **LON-MS1.CONTOSO.COM** and **LON-MS2.CONTOSO.COM**.
- d. Add **SCOM2012_Admins** to the **Operations Manager Administrators** user role.

► **Task 3: Use the Agent Assignment and Failover Wizard**

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Device Management\Management Servers

2. Edit the properties of LON-MS1, and on the **Auto Agent Assignment** tab, add a new Auto Agent Assignment with the following settings (all other settings should remain as the default):
 - 3. Inclusion Criteria: In the **Find Computers** window, in the **Computer name** box, add **LON-AP1**, and then click **Configure**.

► **Task 4: Install the agent using Momagent.msi**

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-AP1
Tool	MOMAgent.msi
Location	\LON-DC1\Media\SCOM2012R2\agent\AMD64

2. Use MOMAgent.msi to install an agent on LON-AP1:
 - a. Cancel the **Connect the agent to System Center Operations Manager** selection during installation

► **Task 5: Confirm the agent is automatically assigned**

1. To perform this task, use the computer and tool information that are shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Device Management\Pending Management

2. Approve **LON-AP1**.
3. Confirm **LON-AP1** is displayed in the **Agent Managed** view.

 **Note:** It can take up to 15 minutes for the agent to appear in the **Pending Management** view.

 **Note:** If after 15 minutes the agent does not appear in the **Pending Management** view on LON-AP1 restart the **Microsoft Monitoring Agent** service and the refresh the **Pending Management** view. If the agent still does not appear perform the following steps on LON-MS1:

1. In the **Operations console** on LON-MS1 click the **Authoring** pane and then expand **Management Pack Objects** and then click **Rules**.
2. From the center pane click **Change Scope**.
3. In the **Scope Management Pack Objects** window that opens click **Clear All** (if it is available) and then click **View all targets**.
4. In the **Look for** box type **AD**.
5. Select the check box for both **AD Assignment Resource Pool** targets and then click **OK**.
6. From the center pane right-click **AD rule for Domain: CONTOSO.COM, ManagementServer: CONTOSO\LON-MS1** and then click **Overrides**, then click **Override this Rule**, then click **For all objects of class: AD Assignment Resource Pool**.
7. In the **Override Properties** window that opens select the **Override** check box for the **Frequency** parameter.
8. In the **Override Value** box for the **Frequency** parameter remove **3600** and then type **300**.
9. Click **OK** on the **Override** window.
10. Wait for **6** minutes and then on LON-AP1 open Windows Services and then restart the **Microsoft Monitoring Agent** service.

Results: After completing this exercise you should have configured Active Directory Integration in Operations Manager. You should have also confirmed that integration is working as expected by manually installing an agent and then confirming that it is automatically assigned to the relevant Management Server.

Exercise 5: Installing and Configuring Audit Collection Services (ACS)

Scenario

To capture failed logon attempts in the Contoso domain, you must first configure the audit policy on a Contoso domain controller. You can then install and configure ACS in Operations Manager and view reports that are based on the data that it collects.

The main tasks for this exercise are as follows:

1. Configure the security event log
2. Install the ACS Collector
3. Configure the ACS Forwarder
4. Configure ACS filtering
5. Configure ACS reporting
6. View ACS reports

► Task 1: Configure the security event log

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-DC1
Tool	Administrative Tools\Local Security Policy
Audit Policy	Audit account Logon events
Setting	Success and Failure

2. Open the local security policy on LON-DC1, and then enable **Success and Failure** auditing for the Audit account logon events policy.

► Task 2: Install the ACS Collector

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Setup.exe
Location	\LON-DC1\Media\SCOM2012R2
Option	Audit collection services

2. From the Operations Manager installation screen, use the **Audit Collection Services** link to install the ACS Collector with the following settings (leave all other default settings):
 - a. Remote database server machine name: **LON-SQ1**
 - b. Database creation options: **Use SQL Servers default data and log file directories**



Note: After completing the **Audit Collection Services Collector Setup Wizard** the installation will fail. This is expected. Open a command prompt and confirm the ADTServer service has started by using the following command:

Net start ADTServer

► Task 3: Configure the ACS Forwarder

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Operations Manager\Agent Details\Agents by Version

- Select **LON-DC1**, and then use the **Enable Audit Collection** task from the **Tasks** pane to enable audit collection on **LON-DC1**.
- Override the tasks, and then add the **LON-MS2.CONTOSO.COM** ACS Collector.

► Task 4: Configure ACS filtering

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Regedt32
Folder	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer
Key	Parameters

- Edit the permissions of the Parameters key, and then enable Full control permission for NETWORK SERVICE.
- Open a Command Prompt window, and then browse to **C:\Windows\System32\Security\ADTServer**.
 - Use the following command to view the current filter.

```
AdtAdmin /getquery
```

- Use the following command to set the filter.

```
AdtAdmin /setquery /query:"SELECT * FROM AdtsEvent WHERE NOT (HeaderUser='SYSTEM')"
```

- Use the following command to view the filter.

```
AdtAdmin /getquery
```

► Task 5: Configure ACS reporting

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	Windows Explorer
Location	\LON-DC1\Media\SCOM2012R2\ReportModels
Folder	ACS

- Copy the **ACS** folder to drive **C** on LON-MS2, open a Command Prompt window, and then browse to the **C:\ACS** folder.
- Run the following command to configure ACS reports.

```
UploadAuditReports LON-SQ1 http://LON-SQ1/ReportServer C:\acs
```

- Open the Operations console, and then confirm that the **Audit Reports** folder is visible in the **Reporting** pane.

► Task 6: View ACS reports

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-DC1
Tool	Windows Logon
Username	Contoso\Administrator
Password	Incorrect password

- Try to log on to LON-DC1 three times by using Contoso\Administrator with an incorrect password.
- Try to log on to LON-DC1 three times with a user name of **FailedLogon** and any password.
- On LON-MS2, from the Operations console, run the **Access_Violation_-_Unsuccessful_Logon_Attempts** report.

Results: After this exercise, you should have installed and configured ACS in System Center 2012 R2 Operations Manager. You should have also configured security event logging on the domain controller LON-DC1 and simulated several failed logon attempts. Finally, you should have viewed the Access_Violation_-_Unsuccessful_Logon_Attempts report to view the failed logon attempts.

Exercise 6: Configuring Agentless Exception Monitoring (AEM)

Scenario

To make it easier to collect error reports for computers that are running in the Contoso domain, you must configure Agentless Exception Monitoring in Operations Manager. You also must confirm that error reports are being collected by creating a simulated application error, and then viewing the data that Operations Manager collects.

The main tasks for this exercise are as follows:

1. Configure a Management Server for client monitoring
2. Configure clients for client monitoring
3. Simulate an exception and view AEM data

► Task 1: Configure a Management Server for client monitoring

1. To perform this task, use the computer and tool information that is shown in the following table

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration\Device Management
View	Management Servers

2. Select LON-MS1, and use the Client Monitoring Configuration Wizard to configure client Monitoring on LON-MS1 by using the following settings (leave all other default settings):
 3. CEIP Forwarding: **Yes, use the selected Management Server to collect and forward CEIP data to Microsoft**
 4. Clear **Use Secure Sockets Layer (SSL) protocol**
 5. File Share Path: **C:\AEM**
 6. Clear **Use Secure Sockets Layer (SSL) protocol**
 7. Error Forwarding: **Forward all collected errors to Microsoft**
 8. Create File Share: **Use the Contoso\Administrator credentials**
 9. Client Settings: **Save the template to the desktop on LON-MS1**
10. Copy the template to the C drive on LON-DC1.

► Task 2: Configure clients for client monitoring

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-DC1
Tool	Administrative Tools\Group Policy Management
Pane	Administration\Device Management
Policy	Default Domain Policy

2. Edit the Default Domain Policy on LON-DC1 and make the following changes:
 - a. Disable the **Turn off Windows Error Reporting policy from Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication Settings**.
 - b. Add the administrative template that was copied in Task 1.
 - c. Turn on the **Configure CEIP (Customer Experience Improvement Program)** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring CEIP Settings**.
 - d. Turn on the **Configure Error Reporting for Windows Vista and later version operating systems** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring**.
 - e. Turn on the **Configure Error Notification** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring**.
 - f. Turn on the **Configure Error Reporting for Windows Operating Systems older than Windows Vista** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring**.
 - g. Turn on the **Application reporting settings (all or none)** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring\Advanced Error Reporting settings**.
 - h. Turn on the **Report operating system errors** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring\Advanced Error Reporting settings**.
3. Turn on the **Report unplanned shutdown events** policy from **Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Applications\System Center Operations Manager (SCOM)\SCOM Client Monitoring\Advanced Error Reporting settings**.

► **Task 3: Simulate an exception and view AEM data**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MS2
Tool	GPUpdate AEMTestApplication
Location	C:\AEMValidation
Parameters	0

2. Open a command prompt on LON-MS2 and then run the following command:

```
gpupdate /force
```

3. Browse to the **C:\AEMValidation** folder and then run the following command.

AEMTestApplication 0

4. Select the **Check online for a solution and close the program** check box.
5. Open the Operations console, and from the **Error Group View** in the **Agentless Exception Monitoring** folder of the **Monitoring pane**, view the **AEMTESTAPPLICATION.EXE** data.
6. Open the **Error Events** view and view the events.
7. Open the **Crash Listener View**, select **LON-MS1**, and then use the **Availability** report task to open the **Availability** report.
8. Change the **From** field to **Yesterday**, and then run the report.
9. Select **Availability Tracker** to view the availability of the AEM Crash Listener.

Results: After this exercise, you should have configured Agentless Exception Monitoring in System Center 2012 R2 Operations Manager. You should also have used the AEMTestApplication utility to simulate an application crash on LON-MS2, and then used views and reports in Operations Manager to view the crash details.

Question:

When you install the Gateway Server feature in System Center 2012 R2 Operations Manager, what is the first step that must be performed?

Question:

When you configure the Gateway Server feature in System Center 2012 Operations Manager, what are the two tools that must be run on the Management Server that will manage the Gateway Server?

Question: You have enabled AEM on a Management Server and have configured the client settings by using the administrative template that is provided by Operations Manager. When application errors occur in the environment, they are not displayed in Operations console. What should you do?

Module Review and Takeaways

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
After installing ACS and configuring ACS reports, you might find no data is displayed when running ACS reports.	

Review Question(s)

Question: You have to deploy an Operations Manager agent to a computer that is in a perimeter network and is protected by a firewall. What should you do?

Real-world Issues and Scenarios

- When you install the first Operations Manager Management Server, if a firewall exists between the Management Server and the computer that is hosting the Operations Manager database, you must open additional firewall ports. You must do this because the installer must connect to the Service Control Manager that runs on the SQL Server to make sure that important SQL services are running. In addition to port 1433 that is open between the Management Server and the Database Server and port 1434 that is open between the database server and the Management Server (if you use a named instance), you must also open the following ports during the installation:
 - RPC: TCP 135
 - NetBIOS: UDP 137, 138, and TCP 139
 - SMB: TCP 445
- After the installation is complete, you can close these ports.

Tools

To filter unwanted security events from the ACS database, you can use the ADTAdmin.exe tool. More details about how to use ADTAdmin.exe can be found here:

<http://go.microsoft.com/fwlink/?LinkID=391265>

Module 3

Upgrading Operations Manager

Contents:

Module Overview	3-1
Lesson 1: Guidelines for Migration and Upgrade to System Center 2012 R2 Operations Manager	3-2
Lesson 2: Upgrading to System Center 2012 R2 Operations Manager	3-5
Lesson 3: Migrating to System Center 2012 R2 Operations Manager	3-14
Lab: Upgrading to System Center 2012 R2 Operations Manager	3-16
Module Review and Takeaways	3-30

Module Overview

If you have already made investments in Microsoft System Center Operations Manager 2007 R2, it is important that you understand the upgrade path from Operations Manager 2007 R2 to Microsoft System Center 2012 R2 Operations Manager.

Upgrading the core components to System Center 2012 R2 Operations Manager can be performed only in an Operations Manager 2007 R2 or newer environment. Earlier versions of Operations Manager, such as Operations Manager 2007 Service Pack 1 (SP1), must be upgraded to Operations Manager 2007 R2 before they can be upgraded to System Center 2012 Operations Manager. Additionally, the Operations Manager 2007 R2 installation must be running at least cumulative update 4.

Before upgrading to System Center 2012 Operations Manager, several important tasks must be performed. In this module, you learn about the upgrade order that should be applied when you upgrade to System Center 2012 Operations Manager.

Before the upgrade to System Center 2012 R2 Operations Manager can be performed, the Management Group must be running System Center 2012 SP1 Operations Manager.

Objectives

After completing this module, students will be able to:

- Plan an upgrade or migration to System Center 2012 R2 Operations Manager.
- Upgrade from Operations Manager 2007 R2 to System Center 2012 R2 Operations Manager.
- Migrate to System Center 2012 R2 Operations Manager.

Lesson 1

Guidelines for Migration and Upgrade to System Center 2012 R2 Operations Manager

If you already have an existing Operations Manager 2007 R2 environment, you must consider a number of factors before deciding whether to upgrade or migrate to System Center 2012 R2 Operations Manager.

Factors could include:

- **Existing version.** You might need to have a staged upgrade approach depending on your current version of Operations Manager.
- **Existing infrastructure.** The current infrastructure that your existing Operations Manager Management Group is installed on might not be supported in System Center 2012 R2 Operations Manager.
- **Custom Management Packs.** You might have a number of custom Management Packs that were developed in your existing Operations Manager environment. These will need to be tested before you import them into a System Center 2012 R2 Operations Manager environment.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe how to plan for an upgrade to System Center 2012 R2 Operations Manager.
- Describe how to plan for a migration to System Center 2012 R2 Operations Manager.

Guidelines for Planning the Upgrade to System Center 2012 R2 Operations Manager

There are many factors that must be considered before deciding to upgrade your existing Operations Manager Management Group to System Center 2012 R2 Operations Manager. Factors are described in the following sections.

Current Version.

Before you can upgrade to System Center 2012 R2 Operations Manager, your existing Operations Manager Management Group must be running at least Operations Manager 2007 R2 Cumulative Update 4. If your Management Group is running an earlier version such as Operations Manager 2007 SP1, your Management Group must be upgraded to Operations Manager 2007 R2 cumulative update 4 first.

Current Infrastructure

You should be aware of the hardware and software requirements for each System Center 2012 R2 Operations Manager component, because the current infrastructure that your existing Management Group is using might not be supported in System Center 2012 R2 Operations Manager. For example, with the exception of the Operations console and the Operations Manager agent, all other System Center 2012 R2 components require 64-bit processor architecture. If any existing Operations Manager component is running on 32-bit processor architecture, this component will need to be moved to a 64-bit server before

Factors that must be considered before upgrade include:

- Current Operations Manager version
- Current infrastructure
- Current deployment
- Upgrade path

it can be upgraded. This process might involve installing a new component such as a secondary Management Server.

Current Deployment

Depending on how your current Operations Manager Management Group is deployed, the process of upgrading to System Center 2012 R2 Operations Manager will differ. For example, if your Operations Manager Management Group is distributed across multiple servers, you must upgrade components such as secondary Management Servers, Gateway Servers, and agents before the Management Group can be upgraded. If all components in your Operations Manager Management Group reside on a single server, all components are upgraded at the same time.

Upgrade Path

You cannot upgrade an Operations Manager 2007 R2 Cumulative Update 4 Management Group to System Center 2012 R2 Operations Manager directly. The following upgrade path must be taken to upgrade an existing Operations Manager 2007 R2 Cumulative Update 4 Management Group to System Center 2012 R2 Operations Manager:

1. Upgrade Operations Manager 2007 R2 Cumulative Update 4 to System Center 2012 Operations Manager.
2. Upgrade System Center 2012 Operations Manager to System Center 2012 SP1 Operations Manager.
3. Upgrade System Center 2012 SP1 Operations Manager to System Center 2012 R2 Operations Manager.

For further information about upgrading Operations Manager 2007 R2 to System Center 2012 Operations Manager, visit the following website.



Upgrading from System Center Operations Manager 2007 R2

<http://go.microsoft.com/fwlink/?LinkID=391266>

Guidelines for Planning Migration to System Center 2012 R2 Operations Manager

If you plan to migrate to System Center 2012 R2 Operations Manager, you do not need to upgrade the existing environment to System Center 2012 Operations Manager or System Center 2012 SP1 Operations Manager first. Instead, you install a new System Center 2012 R2 Operations Manager Management Group and manage the same computers and devices that the existing Operations Manager 2007 R2 Management Group manages. One key benefit in migration is that you can test features and functionality in the new System Center 2012 R2 Management Group before turning off any monitoring in the existing Operations Manager 2007 R2 Management Group.

As described in the section “Guidelines for Planning the Upgrade to System Center 2012 R2 Operations Manager” earlier in this module, there are also key factors that must be considered when deciding to migrate to System Center 2012 R2 Operations Manager. These factors are described in the following sections.

Factors that must be considered before migration include:

- Provisioning of the new infrastructure
- The plan for upgrading existing agents
- Testing of new features and functionality

Provisioning New Infrastructure

Because you will be installing a new System Center 2012 R2 Operations Manager Management Group, you need to provision new servers for the Management Group components. You also need to make sure that the new servers meet the hardware and software requirements of System Center 2012 R2 Operations Manager. In addition, you need to decide whether to deploy a single or distributed Operations Manager Management Group.

Upgrading Agents

For the existing Operations Manager agents to communicate with the new System Center 2012 R2 Management Group, you will need to upgrade them. This is because a System Center 2012 R2 agent can communicate with both an Operations Manager 2007 R2 Management Group and a System Center 2012 R2 Management Group. However, an Operations Manager 2007 R2 agent cannot communicate with a System Center 2012 R2 Management Group.

Testing New Features and Functionality

You should create a checklist of features and functionality to test in the new System Center 2012 R2 Operations Manager environment. This will ensure that any existing monitoring that is performed in the Operations Manager 2007 R2 environment is replicated in the System Center 2012 R2 environment. Additionally, you should test any custom Management Packs in the new environment, because further development might be required before they can be used.

Question: You are planning to upgrade your existing Operations Manager 2007 R2 Management Group to System Center 2012 Operations Manager. What is the minimum Cumulative Update that must be applied to the Operations Manager 2007 R2 environment?

Lesson 2

Upgrading to System Center 2012 R2 Operations Manager

When upgrading to System Center 2012 R2 Operations Manager from previous versions of the product, you should be aware of the important preupgrade tasks that must be completed to prepare the environment for upgrade. These tasks also differ depending on whether you currently have a single or distributed Operations Manager Management Group. In addition, when performing the upgrade, it is important to know in which order each component is upgraded.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe how to prepare the Operations Manager environment for upgrade.
- Describe how to upgrade the Operations Manager 2007 R2 environment to System Center 2012 Operations Manager.
- Describe how to upgrade System Center 2012 Operations Manager to System Center 2012 SP1 Operations Manager.
- Describe how to upgrade System Center 2012 SP1 Operations Manager to System Center 2012 R2 Operations Manager.

Guidelines for Preparing the Operations Manager Management Group for Upgrade

Before you upgrade to System Center 2012 Operations Manager, you must perform a series of tasks in the Operations Manager 2007 R2 environment to make sure that the upgrade completes without any issues.

You must perform the following tasks before you can upgrade a distributed Operations Manager 2007 R2 Management Group:

- **Confirm the infrastructure is ready to upgrade.** When you reference the "System Requirements for System Center 2012 - Operations Manager" TechNet article as you plan, you should make sure that the infrastructure servers hosting the Operations Manager 2007 R2 Management Group have the necessary hardware and software prerequisites.

Preparing the Operations Manager 2007 R2 environment includes:

- Confirming the infrastructure is prepared and ready
- Importing the Upgrade Helper Management Pack
- Moving the agents that report to RMS to a secondary Management Server
- Backing up the encryption key
- Reviewing the Operations Manager 2007 R2 event logs
- Removing agents from pending management
- Verifying SQL Server collation



The TechNet article "System Requirements for System Center 2012 - Operations Manager" can be found here:

System Requirements for System Center 2012 - Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=391267>

- **Import the Upgrade Helper Management Pack.** The Upgrade Helper Management Pack is useful for confirming a successful upgrade to Operations Manager 2012. The Management Pack creates views that show each component's upgrade status. These views should be used at each stage of the upgrade to confirm the upgrade status of each component.

- **Move agents that report to the root management server (RMS) to a secondary Management Server.** Although this task is optional, it should be performed to make sure that there is no downtime of the monitored environment during the upgrade.
- **Back up the encryption key.** The RMS encryption key is used to encrypt data that is stored in the operational database. The key can be used on a new Management Server when you upgrade the Management Group from an Operations Manager 2007 R2 Management Server.
- **Review the Operations Manager 2007 R2 event logs.** View the Operations Manager event log on the RMS and on any secondary Management Servers. You must resolve any critical or warning events that occur in the environment before you can start an upgrade to Operations Manager 2012.
- **Remove agents from pending management.** For the manually installed agent to be upgraded successfully, there should be no agents in the Pending Management view. You should either approve or reject any agents that are in pending management.
- **Verify that your Microsoft SQL Server collation is supported.** Operations Manager 2012 supports SQL_Latin1_General_CI_AS collation in SQL server. You should make sure that all databases and database instances are configured by using this collation. This is for the English-language versions.

More information about pre-upgrade tasks for Operations Manager can be found on the following link:

Pre-Upgrade Tasks for Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=321849>

The Process of Upgrading from Operations Manager 2007 R2 to System Center 2012 Operations Manager

You perform the following tasks, in order, when you upgrade a distributed Operations Manager 2007 R2 Management Group to System Center 2012 Operations Manager.

Task 1: Upgrade manually installed agents

Log on, as a local administrator, to the computers that have an Operations Manager 2007 R2 manually installed agent. Then, run Setup.exe from the Operations Manager 2012 media. Click the Local agent option in the setup wizard to upgrade the manually installed agent. You can also use upgrade an agent by using the following command.

```
msiexec /i MOMAgent.msi /qn /l*v D:\Logs\AgentUpgrade.log
```

Upgrading the Operations Manager 2007 R2 environment includes:

- Upgrading manually installed agents
- Upgrading secondary Management Servers
- Upgrading Gateway Servers
- Upgrading push-installed agents
- Upgrading the RMS
- Upgrading the Web console and Reporting Server



After the agent is upgraded, you can use the Agent Managed view in the Administration pane in the Operations console to verify that the agent is upgraded successfully. The version column for the agent should display 7.0.8560.0.

Task 2: Upgrade secondary Management Servers

Log on as Operations Manager Administrator to the computers that have an Operations Manager 2007 R2 secondary Management Server installed. Then, run Setup.exe from the Operations Manager 2012 media. In the setup window that opens, click the Install option. During the upgrade, you will receive a message asking for the System Center Configuration service and the System Center Data Access service accounts. Domain accounts should be specified here as described in the topic "Operations Manager Security Accounts" in module 1. To verify that the secondary management servers are upgraded successfully, you can use the Management Servers view in the Administration pane. Then you can confirm the version of the Management Server is displayed as 7.0.8560.0.

Task 3: Upgrade Gateway Servers

To upgrade the Gateway Servers, you log on to the servers as an Operations Manager Administrator. Then, run Setup.exe from the Operations Manager 2012 media. Click the Gateway Management Server option from the optional Installations section. You can verify that the Gateway Servers are upgraded successfully by using the same method that is used for Management Servers.

Task 4: Upgrade push-installed agents

To upgrade push-installed agents, you first log on to the server that is hosting the 2012 Operations console. Open the console as an Operations Manager Administrator. In the Administration pane, under Device Management, click the Pending Management view. Agents will be listed with a status of Agent Requires Update. Right-click each agent, and then click Approve to upgrade the agents. Enter the administrator account credentials that will be used by the upgrade process. The agent upgrade status is shown in the Agent Management Task Status dialog box. One best practice is to not approve more than 200 agents in any one operation. As soon as the upgrade has completed, you can view the Agents status by using the Agent Managed view in the Administration pane. The version of the agent should be displayed as 7.0.8560.0.

Task 5: Check for any active, connected consoles to the root management server

During the upgrade of the RMS, any console connections to the RMS will be disconnected. Therefore, it is advised that all users who have an active console connection close the Operations console.

Task 6: Disable all notification subscriptions

To make sure that the notifications are not sent during the upgrade, disabling all notification subscriptions is recommended. In the Administration pane, in the Operations console, click Subscriptions under the Notifications container, and then for each subscription, click the Disable option from the Actions pane to disable the notification subscription.

Task 7: Stop services or disable any connectors that are installed

Any connectors that are run in the Operations Manager 2007 R2 environment should be disabled before the upgrade to the RMS is performed. This helps make sure that no errors are generated, because the connection is unavailable during the upgrade.

Task 8: Verify that your operational database has sufficient free space

The operational database must have a minimum of 50 percent free space before the Management Group is upgraded, or the upgrade will fail. You should also make sure that the size of the transaction logs are set to a minimum of 50 percent of the operational database.

Task 9: Back up the databases

As with any upgrade, you should make sure there is an up-to-date backup and that it is verified before the upgrade is performed. You should back up the operational database and the data warehouse database. You should also back up the reporting services database and the Audit Collection Services (ACS) database, if this is applicable.

Task 10: Restore the encryption key on the secondary Management Server

If the RMS in the Operations Manager 2007 R2 environment does not meet the prerequisites for Operations Manager 2012 or the RMS is clustered, you might have to restore the RMS encryption key on a secondary Management Server to upgrade the Management Group. The following command line can be used to restore the RMS encryption key on the secondary Management Server.

```
SecureStorageBackup Restore <BackupFile>
```

Task 11: Run Management Group upgrade on the RMS

Upgrading the Operations Manager 2007 R2 RMS is the process in which the Management Group is upgraded to Operations Manager 2012. To upgrade the RMS, you must log on to the server that hosts the RMS and run Setup.exe from the Operations Manager 2012 media. On the setup screen, you then click the Install option. The account that you use to log on to the server must be a member of the Operations Manager Administrators role. During the upgrade, you are prompted for the System Center Configuration service and System Center Data Access service account.

Task 12: Upgrade any additional features that are enabled

After you upgrade the RMS, additional features such as stand-alone consoles, web consoles, reporting and ACS collectors can be upgraded. To upgrade each feature, you log on to the relevant server as an Operations Manager Administrator, and then from the Operations Manager 2012 media you run Setup.exe. Then you select the Install option from the setup screen, and follow the instructions to upgrade the feature.

Task 13: Re-enable notification subscriptions

After the upgrade is complete, notification subscriptions can be re-enabled. You follow the same procedure to disable notification subscriptions described earlier, except that in the Actions pane, you select the Enable task.

Task 14: Restart or re-enable the service for any connectors that are installed

You can restart the connector services after the upgrade to enable data flow between the connected environment and the Management Group environment to continue.

Task 15: Update overrides

If there are any overrides for the Active Directory Integration rules, they must be deleted and recreated in the upgraded environment. The overrides must target the Active Directory Assignment resource pools appropriately.

Task 16: Verify the success of the upgrade

To verify a successful upgrade to Operations Manager 2012, the following tasks should be performed:

1. From the Operations console, in the **Administration** pane, confirm that the Management Servers and agents are reporting as healthy.
2. In the **Monitoring** pane, review the **Active Alerts** view and check for any alerts that relate to the health of the Management Group.
3. View the Operations Manager event log on all Management Servers and Gateway Servers, and check for new errors.
4. Check the CPU and disk I/O levels on the database servers to make sure that they are operating at expected levels.
5. In the **Reporting** pane, in the Operations console, make sure that the reports are functioning as expected.

6. Review the **Upgrade Helper Management Pack** views. In the **Monitoring** pane, expand **Operations Manager Upgrade Management Pack** and use the following views to confirm each component is upgraded successfully and displays a healthy state:

- **Step 1: Upgrade Secondary Management Servers**
- **Step 2: Upgrade Gateway Servers**
- **Step 3a: Upgrade Windows Agents**
- **Step 3b: Upgrade Unix/Linux Agents**
- **Step 4: Upgrade Root Management Server and Databases**

More information about how to upgrade to System Center 2012 Operations Manager can be found on the following link:

 **Upgrading to System Center 2012 - Operations Manager**

<http://go.microsoft.com/fwlink/?LinkId=321850>

To review a flow diagram for the process of upgrading to System Center 2012 Operations Manager, visit the following link:

 **System Center 2012 - Operations Manager Upgrade Process Flow Diagram**

<http://go.microsoft.com/fwlink/?LinkId=321851>

The Process of Upgrading from System Center 2012 Operations Manager to System Center 2012 SP1 Operations Manager

Before upgrading a System Center 2012 Operations Manager Management Group to System Center 2012 SP1 Operations Manager, there are a number of preupgrade tasks that must be performed. In the following table, each preupgrade task is described. The order in which the tasks are presented in the table is the order in which they should be performed.

When upgrading to System Center 2012 SP1 Operations Manager, the upgrade order is as follows:

1. Management servers (including ACS collectors)
2. Gateway servers
3. Stand-alone consoles
4. Agents
5. Web console server
6. Reporting server

Pre-upgrade task	Description
Review the Operations Manager event logs	You should review the Operations Manager event logs on all Management Servers and resolve any critical or warning events that are occurring.
Clean up the (extract, transform and load ETL table	<p>During the upgrade to System Center 2012 SP1 Operations Manager, a script is run to clean up the ETL tables. In some cases where there are greater than 100,000 rows to clean up, the setup procedure can either stop responding or time-out. For this reason, it is recommended to manually perform the cleanup task by using an SQL query. The following query can be used to determine the number of rows that will be deleted during the cleanup procedure.</p> <pre data-bbox="714 614 1383 931">DECLARE @SubscriptionWatermark bigint = 0; SELECT @SubscriptionWatermark = dbo.fn_GetEntityChangeLogGroomingWatermark(); Select COUNT (*) FROM EntityTransactionLog ETL with(nolock) WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL with(nolock) WHERE ECL.EntityTransactionLogId = ETL.EntityTransactionLogId) AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL with(nolock) WHERE RECL.EntityTransactionLogId = ETL.EntityTransactionLogId) AND EntityTransactionLogId < @SubscriptionWatermark;</pre> <p>The cleanup procedure can then be run by using the following SQL query.</p> <pre data-bbox="714 1015 1400 1543">DECLARE @RowCount int = 1; DECLARE @BatchSize int = 100000; DECLARE @SubscriptionWatermark bigint = 0; DECLARE @LastErr int; SELECT @SubscriptionWatermark = dbo.fn_GetEntityChangeLogGroomingWatermark(); WHILE(@RowCount > 0) BEGIN DELETE TOP (@BatchSize) ETL FROM EntityTransactionLog ETL WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL WHERE ECL.EntityTransactionLogId = ETL.EntityTransactionLogId) AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL WHERE RECL.EntityTransactionLogId = ETL.EntityTransactionLogId) AND ETL.EntityTransactionLogId < @SubscriptionWatermark; SELECT @LastErr = @@ERROR, @RowCount = @@ROWCOUNT; END</pre>
Remove agents from pending management	If any Operations Manager agents are in pending management, they should either be approved or rejected before the upgrade is started.
Disable notification subscriptions	To ensure that notifications are not sent as a result of services being restarted, you should disable any notification subscriptions.
Stop or disable any connectors	To temporarily suspend any communication during the upgrade, you should either disable any connectors or stop the service that they use.

Verify the operational database size	The operational database must have at least 50 percent free space available or the upgrade procedure might fail. You should also ensure that the transaction logs are 50 percent of the total size of the operational database.
Back up the Operations Manager databases	You should ensure a recent (verified) backup of both the operational and data warehouse databases have been performed.

After performing the preupgrade tasks, you can then perform the upgrade to System Center 2012 SP1 as described in the following sections.

Task 1: Upgrade the Management Servers

When upgrading a distributed Operations Manager Management Group, you must first upgrade the Management Servers. In addition, you must wait until the upgrade of each Management Server completes before starting the upgrade of the next. If the Management Server also hosts an ACS collector server, this must be upgraded by using the Install ACS Collector Server option in the Operations Manager setup window.

Task 2: Upgrade the Gateway Servers

After the Management Servers have been upgraded, any Gateway Servers must then be upgraded. When running setup from the System Center 2012 SP1 Operations Manager media on a Gateway Server, click the Upgrade option.

Task 3: Upgrade Any Stand-alone Operations Consoles

If any stand-alone Operations consoles are deployed, these consoles can be upgraded by using the Install option from the System Center 2012 SP1 media. Setup detects the presence of the Operations console, and the Upgrade option is then selected. Any Operations consoles that are installed on Management Servers will be upgraded as part of the Management Server upgrade.

Task 4: Upgrade Agents

Agents that were deployed by using the console (Push) method can be upgraded by using the Pending Management view in the Administration pane of the Operations console. For each agent that should be upgraded, you select the Approve option in the Tasks pane. For manually installed agents, you run Setup from the System Center 2012 SP1 Operations Manager media and then select the Local Agent option. Setup detects the presence of the agent, and then the Upgrade option is clicked.

Task 5: Upgrade the Web Console

The Web console can be upgraded by running Setup from the System Center 2012 SP1 Operations Manager media on the Web console server. Setup detects the presence of the Web console server, and then the Upgrade option is selected.

Task 6: Upgrade the Reporting Server

The reporting server can be upgraded by running Setup from the System Center 2012 SP1 Operations Manager media on the Web console server. Setup detects the presence of the reporting server, and then the Upgrade option is selected.

Task 1: Post-Upgrade tasks

After upgrading all components within the Management Group to System Center 2012 SP1, the following post-upgrade tasks should be performed:

- Re-enable Notification Subscriptions.
- Restart any connector services or re-enable the connectors.

- On agents where an ACS Forwarder is installed, re-enable the ACS service.
- Verify a successful upgrade by performing the following steps:

Verify the health state for each Management Server by using the Health Service Watcher state view in the Administration pane of the Operations console.

Review the Operations Manager event logs on the Management Servers.

Check for any new alerts in the Active Alerts view that relate to the Management Group health.

Ensure reports work as expected.

If any agents were uninstalled during the upgrade process, redeploy them.

The Process of Upgrading from System Center 2012 SP1 Operations Manager to System Center 212 R2 Operations Manager

The processes involved when upgrading from System Center 2012 SP1 Operations Manager to System Center 2012 R2 Operations Manager are almost identical to the processes involved when upgrading from System Center 2012 Operations Manager to System Center 2012 SP1 Operations Manager.

The preupgrade tasks and upgrade order is the same as described in the section "The Process of Upgrading from System Center 2012 Operations Manager to System Center 2012 SP1 Operations Manager" earlier in this module, so only the high-level steps are included in the following lists.

When upgrading to System Center 2012 R2 Operations Manager, the upgrade order is as follows:

1. Management servers (including ACS collectors)
2. Gateway servers
3. Stand-alone consoles
4. Agents
5. Web console server
6. Reporting server

Preupgrade Tasks

- Review the Operations Manager event logs.
- Cleanup the ETL table.
- Remove agents from pending management.
- Disable notification subscriptions.
- Stop or disable any connectors.
- Verify the operational database size.
- Back up the Operations Manager databases.

Upgrade Tasks

1. Upgrade the Management Servers.
2. Upgrade the Gateway Servers.
3. Upgrade any stand-alone Operations consoles.
4. Upgrade agents.
5. Upgrade the Web console.
6. Upgrade the Reporting server.

7. Perform post-upgrade tasks.

Question: When upgrading from System Center 2012 SP1 to System Center 2012 R2, what is the first component to be upgraded?

Demonstration: Upgrading Operations Manager 2007

In this demonstration, you will learn how to upgrade an Operations Manager 2007 Management Group to System Center 2012 Operations Manager.

Demonstration Steps

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MG1
Tool	Operations Manager Setup
Location	\LON-DC1\Media\SCOM2012
Setup file	Setup.exe

2. Upgrade Operations Manager by accepting all default values.
3. On the **Configure Operations Manager accounts page**, use the **Contoso\svc_SCOM2007_das** account by using the password **Pa\$\$w0rd**.
4. Cancel the wizard before performing the upgrade.

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
You can upgrade from Operations Manager 2007 R2 cumulative update 4 to System Center 2012 SP1 Operations Manager?	

Lesson 3

Migrating to System Center 2012 R2 Operations Manager

In many scenarios, you might prefer, or you might be required, to migrate to a new System Center 2012 R2 Operations Manager Management Group instead of upgrading from a previous version. For example, your Operations Manager 2007 R2 environment might include Management Servers that use 32-bit processor architecture. In this scenario, an upgrade is not possible, because System Center 2012 R2 Operations Manager requires Management Servers to be installed on 64-bit processor architecture and a 64-bit operating system.

Another reason you might prefer to migrate instead of performing an upgrade is to test functionality with the new version before removing the former version. In such a case, custom Management Packs might have been deployed in an Operations Manager 2007 R2 Management Group, and you need to test that functionality works as expected before importing the Management Packs into the System Center 2012 R2 Management Group.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe how to ensure System Center 2012 R2 Operations Manager and Operations Manager 2007 R2 successfully coexist.
- Describe how to migrate from Operations Manager 2007 R2 to System Center 2012 R2 Operations Manager.

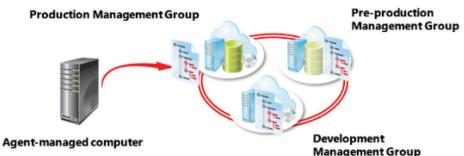
Coexistence of System Center Operations Manager 2007 R2 and System Center 2012 R2 Operations Manager

In this scenario, System Center Operations Manager 2007 R2 is currently used in production to provide all monitoring and reporting functions for the organization.

A new System Center 2012 R2 Operations Manager Management Group is deployed in the environment by using new servers to host the relevant components that are required. As soon as the new Management Group is deployed and functional, a new Operations Manager agent is deployed to computers that are currently being monitored by Operations Manager 2007 R2.

Multi-homing the Operations Manager agent

- Up to four Management Groups
- Monitored data sent to each Management Group
- Useful for having two different Operations Manager versions coexist
- Useful for preproduction/production environments



When a computer hosts the Operations Manager agent for more than one Management Group, the term that is used to describe this function is named multihomed. In both Operations Manager 2007 R2 and System Center 2012 R2 Operations Manager, a computer that is hosting the Operations Manager agent can multihome up to four Management Groups.

When you use the multihoming feature, the Operations Manager agent sends monitored data back to Management Servers in different Management Groups at the same time.

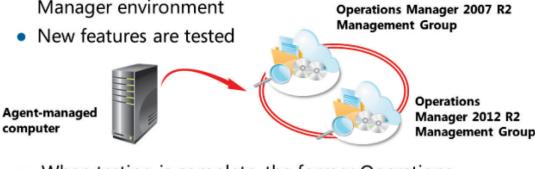
The multihome feature is useful for both coexisting different versions of Operations Manager and for organizations that want to follow a preproduction (or test) Management Group and a production Management Group. This feature lets you test Management Packs and their effect in a test environment before you deploy the Management Packs to the production environment.

Considerations When Migrating from Operations Manager 2007 R2 to System Center 2012 R2 Operations Manager

For migration purposes, the multihome feature discussed in the previous topic also means that there is no downtime of monitoring, because agents continue to report to both Management Groups before and during the migration.

Management Packs that are deployed in each Management Group continue to function as before and are completely separate. This means that agents send data back only to their respective Management Group. Data is not passed between Management Groups.

During migration, the following tasks can be performed:

- Agents are multi-homed between both Operations Manager environments
 - Management Packs are tested in the new Operations Manager environment
 - New features are tested
- 
- When testing is complete, the former Operations Manager environment is decommissioned

During migration, Management Packs can be exported from the Operations Manager 2007 R2 environment and tested in the System Center 2012 R2 Operations Manager environment. During this phase, the multihomed agent sends the same monitored data back to both Management Groups. New features such as application performance monitoring (APM) can also be tested during this phase.

In the scenario where the Operations Manager agent sends monitored data to both an Operations Manager 2007 R2 Management Group and a System Center 2012 R2 Operations Manager Management Group, the agent must first be upgraded to Operations Manager 2012. This must occur because the Operations Manager 2012 R2 agent can communicate with the Operations Manager 2007 R2 Management Group. However, the Operations Manager 2007 R2 agent cannot communicate with the Operations Manager 2012 R2 Management Group.

When testing is complete and it is confirmed that the new System Center 2012 R2 Operations Manager Management Group is providing the level of monitoring that is required, the former System Center 2007 R2 environment can be decommissioned.

Be aware that in this scenario, all historical data that is stored in the Operations Manager data warehouse will be lost when the former Operations Manager 2007 R2 Management Group is decommissioned. If you must keep this data, an upgrade path should be considered instead of migration.

Question: You want to test some new features of System Center 2012 R2 Operations Manager in your preproduction environment before you upgrade from Operations Manager 2007 R2. What can you do to make this easier while you still maintain the Operations Manager 2007 R2 environment?

Lab: Upgrading to System Center 2012 R2 Operations Manager

Scenario

Contoso, Ltd., has an existing Operation Manager 2007 R2 environment that must be upgraded to System Center 2012 R2 Operations Manager. You must first prepare the environment by performing the various preupgrade tasks. You must then perform an upgrade to System Center 2012 Operations Manager. After the upgrade to System Center 2012 Operations Manager has completed, you must then upgrade the Management Group to System Center 2012 SP1 Operations Manager. Finally, you must then upgrade the Management Group to System Center 2012 R2 Operations Manager.

Objectives

After completing this lab, you will be able to:

- Prepare an Operations Manager 2007 R2 environment for an upgrade to System Center 2012 Operations Manager.
- Upgrade an Operations Manager 2007 R2 Management Group to System Center 2012 Operations Manager.
- Upgrade an Operations Manager 2012 Management Group to System Center 2012 SP1 Operations Manager.
- Upgrade an Operations Manager 2012 SP1 Management Group to System Center 2012 R2 Operations Manager.

Lab Setup

Estimated Time: 120 minutes

Virtual Machines: 10964C-LON-DC1, 10964C-LON-RMS, 10964C-LON-MG1

User Name: Contoso\Administrator

Password: Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, in Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:
 - 10964C-LON-RMS
 - 10964C-LON-MG1



Note: Before starting this lab, make sure that all Windows Services that are set to start automatically are running, except for the Microsoft .NET Framework NGEN v4.0.30319_X86 and .NET Framework NGEN v4.0.30319_X64 services, because these services stop automatically when they are not in use.



Note: The following exercises in this lab are optional:

- Upgrading the System Center 2012 Management Group to System Center 2012 SP1
- Upgrading the System Center 2012 SP1 Management Group to System Center 2012 R2 Operations Manager

Exercise 1: Preparing the Operations Manager 2007 R2 Environment for Upgrade

Scenario

There are several preupgrade tasks that must be completed to ensure that your Operations Manager 2007 R2 environment is ready to be upgraded. These include checking that the desired Cumulative Update is installed (this must be a minimum of Cumulative Update 4), and making sure that your agents are not connected to the RMS (these should be redirected to a primary Management Server). You must also back up the RMS encryption key and restore it on any Management Servers you are going to upgrade.

The main tasks for this exercise are as follows:

1. Confirm the Operations Manager version
2. Import the Upgrade Helper management pack
3. Move agents that report to the RMS to a secondary Management Server
4. Back up the encryption key
5. Review the Operations Manager 2007 R2 event logs
6. Remove agents from pending management
7. Verify SQL Server and database collation
8. Verify that the operational database has enough free space
9. Backup the Operations Manager databases
10. Restore the encryption key on the secondary Management Server

► Task 1: Confirm the Operations Manager version

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Monitoring
View	Agents by Version

2. Confirm the **Patch List** for LON-DC1 displays **CU5**.

3. View the properties of the **HealthService.dll** file that is located in the **C:\Program Files\System Center Operations Manager 2007** folder, and then confirm the **File Version** displays **6.1.7221.81**.

► **Task 2: Import the Upgrade Helper management pack**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Copy the **OperationsManager.Upgrade.mp** Management Pack from **\LON-DC1\Media\SCOM2012\MANAGEMENTPACKS** to the desktop of **LON-RMS**
3. In the **Actions** pane, use the Import Management Packs wizard to import the **OPERATIONSMANAGER.UPGRADE.MP management pack**.
4. Confirm the Management Pack is successfully imported by viewing the **Monitoring\ Operations Manager Upgrade MP** views.

► **Task 3: Move agents that report to the RMS to a secondary Management Server**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Administration
View	Device Management\Agent Managed

2. Using the **Change Primary Management Server** action from the **Actions** pane, change the primary Management Server for LON-DC1 to **LON-MG1**.

► **Task 4: Back up the encryption key**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Administrator Command Prompt
Command	SecureStorageBackup
Parameters	Backup

2. At the command prompt, browse to **C:\Program Files\System Center Operations Manager 2007**, and then execute the following command by using the **Administrator** password when you are prompted.

```
SecureStorageBackup Backup c:\encryptionkey.snk
```

► **Task 5: Review the Operations Manager 2007 R2 event logs**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS LON-MG1
Tool	Event Viewer
Event log	Operations Manager
Events	Warning, Error or Critical

2. View the **Operations Manager** event logs and review any warning, error or critical events.

► **Task 6: Remove agents from pending management**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Administration
View	Device Management\Pending Management

2. Confirm there are no computers in **Pending Management**.

3. If **LON-DC1** is listed, use the **Approve** task to approve it.

► **Task 7: Verify SQL Server and database collation**

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	SQL Server Management Studio
Databases	OperationsManager
Query	SELECT DATABASEPROPERTYEX ('OperationsManager','collation') SQLcollation

- Execute a new query by using the details that are described earlier and confirm that the **SQL Collation** is set to **SQL_Latin1_General_CI_AS**.

► **Task 8: Verify that the operational database has enough free space**

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	SQL Server Management Studio
Databases	OperationsManager
Properties	Size Space Available

- View the properties of the **OperationsManager** database, and by using the **Size** and **Space Available** fields, determine whether there is more than 50 percent of free space available.
- Using the **Files** tab in the OperationsManager database properties increase **MOM_DATA** to **1500**.

► **Task 9: Backup the Operations Manager databases**

- To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	SQL Server Management Studio
Databases	OperationsManager OperationsManagerDW
Task	Back up

- Using the **Back Up** task, back up **OperationsManager** and **OperationsManagerDW** by using default backup parameters.

► **Task 10: Restore the encryption key on the secondary Management Server**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MG1
Tool	Administrator Command Prompt
Command	SecureStorageBackup
Parameters	Restore

2. Copy the **encryptionkey.snk** file that you created in the "Back up the encryption key" task to drive C on LON-MG1.
3. On LON-MG1, at a command prompt, browse to **C:\Program Files\System Center Operations Manager 2007**, and then execute the following command by using the **Administrator** password when you are prompted.

```
SecureStorageBackup Restore c:\encryptionkey.snk
```

Results: After this exercise, you should have performed the necessary preupgrade tasks for Center Operations Manager 2007 R2 upgrade in this environment. You should know the preupgrade tasks and the order in which they are performed for this specific environment. The tasks and order in other environments could be different based on how Operations Manager 2007 R2 is deployed.

Exercise 2: Upgrading the Operations Manager 2007 R2 Management Group to System Center 2012 Operations Manager

Scenario

After completing the preupgrade tasks in the “Preparing the Operations Manager 2007 R2 Environment for upgrade” exercise, you are now ready to continue with the upgrade to System Center 2012 Operations Manager. The secondary Management Servers and agents are upgraded before the RMS. It should also be noted that other upgrade steps might need to take place that are not covered in this exercise, because the relevant components of the product are not used, such as ACS or manually installed agents.

The main tasks for this exercise are as follows:

1. Upgrade the secondary Management Server
2. Upgrade the push-installed agents
3. Check for any active connected consoles to the RMS
4. Run the Management Group upgrade on the RMS
5. Verify the success of the upgrade

► Task 1: Upgrade the secondary Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MG1
Tool	Operations Manager Setup
Location	\\\LON-DC1\Media\SCOM2012
Setup file	Setup.exe

2. Delete the **AgentManagement** folder that is located in C:\Program Files\System Center Operations Manager 2007\.
3. Upgrade Operations Manager by accepting all default values.
4. On the **Configure Operations Manager accounts** page, add the **Contoso\svc_SCOM2007_das** account using the password **Pa\$\$w0rd**.

► Task 2: Upgrade the push-installed agents

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Administration
View	Device Management\Pending Management

2. Refresh the view, and use the **Approve** action to approve the upgrade for LON-DC1.
3. When you run the task, click the **Other user account** option, and then enter the **Administrator** credentials.
4. If the upgrade fails, reject **LON-DC1** in the **Pending Management** view, and then delete **LON-DC1** in the **Agent Managed** view.

► **Task 3: Check for any active connected consoles to the RMS**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Performance Monitor
Counter	OpsMgr SDK Service
Object	Client Connections

2. Use Performance Monitor to confirm that there are active client connections to the RMS.

► **Task 4: Run the Management Group upgrade on the RMS**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Manager Setup
Location	\LON-DC1\Media \LON-DC1\Media\SCOM2012
Setup file	ReportViewer.exe Setup.exe

2. Delete the **AgentManagement** folder that is located in C:\Program Files\System Center Operations Manager 2007\.
3. Install **ReportViewer** by using default settings.
4. Upgrade Operations Manager by accepting all default settings.
5. On the **Configure Operations Manager** accounts page, use the **Contoso\svc_SCOM2007_das** account for the **System Center Configuration service** and **System Center Data Access** service account using the password **Pa\$\$w0rd**.

► **Task 5: Verify the success of the upgrade**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Monitoring
View	Operations Manager Upgrade MP\Step 4: Upgrade Root Management Server and Databases (Upgrade Helper MP)

2. Confirm that LON-RMS is visible and in a healthy state.

Results:

After this exercise, you should have performed an upgrade of the existing Operations Manager 2007 R2 environment to System Center 2012 Operations Manager. This includes the secondary Management Server, agents, and RMS. By using the Operations Manager Upgrade Management Pack, you confirmed that the RMS upgraded successfully.

Exercise 3: Upgrading the System Center 2012 Management Group to System Center 2012 SP1

Scenario

With the Operations Manager Management Group successfully upgraded to System Center 2012 Operations Manager, the Management Group can now be upgraded to System Center 2012 SP1 Operations Manager. This upgrade is required before an upgrade to System Center 2012 R2 Operations Manager can be performed.

The main tasks for this exercise are as follows:

1. Prepare the System Center 2012 Operations Manager environment
2. Upgrade the first Management Server
3. Upgrade the second Management Server
4. Verify the success of the upgrade

► Task 1: Prepare the System Center 2012 Operations Manager environment

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Microsoft SQL Server Management Studio
Database	OperationsManager
Query	C:\CheckETL.txt C:\CleanETL.txt

2. Copy the contents of the **CheckETL.txt** file into a new query window, and then execute the query against the **OperationsManager** database.
3. Copy the contents of the **CleanETL.txt** file into a new query window, and then execute the query against the **OperationsManager** database.
4. Close Microsoft SQL Server Management Studio.
5. On LON-MG1, open the registry, and then browse to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup.
6. Edit the following keys as follows:
 - DataWarehouseDBName: **OperationsManagerDW**
 - DataWarehouseDBServerName: **LON-RMS**

► Task 2: Upgrade the first Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MG1

Location	Value
Tool	Setup.exe
Location	\LON-DC1\Media\SCOM2012SP1

2. Restart LON-MG1.
3. Run the System Center 2012 – Operations Manager Upgrade wizard to upgrade the Management Server.
4. On the **Configure Operations Manager accounts** page, use the following **Domain Account** credentials:
 - Domain\User Name: **Contoso\svc_SCOM2007_das**
 - Password: **Pa\$\$w0rd**
5. Accept all other default settings.

► Task 3: Upgrade the second Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Setup.exe
Location	\LON-DC1\Media\SCOM2012SP1

2. Restart LON-RMS
3. Run the System Center 2012 – Operations Manager Upgrade wizard to upgrade the Management Server.
4. On the **Configure Operations Manager accounts** page, use the following **Domain Account** credentials:
 - Domain\User Name: **Contoso\svc_SCOM2007_das**
 - Password: **Pa\$\$w0rd**
5. Accept all other default settings.

► Task 4: Verify the success of the upgrade

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Administration
View	Management Servers

2. Confirm that LON-RMS and LON-MG1 are in a healthy state.
3. Run the **Management Group** report from the Microsoft ODR Report Library, folder and confirm the report is generated as expected.
4. Close the Operations console.

Results: After this exercise, you should have upgraded the Operations Manager Management Group to System Center 2012 SP1 Operations Manager. You should have also confirmed that the Management Group is operating as expected.

Exercise 4: Upgrading the System Center 2012 SP1 Management Group to System Center 2012 R2 Operations Manager

Scenario

The Management Group is successfully upgraded to System Center 2012 SP1 Operations Manager and can now be upgraded to System Center 2012 R2 Operations Manager.

The main tasks for this exercise are as follows:

1. Upgrade the first Management Server
2. Upgrade the second Management Server
3. Verify the success of the upgrade

► Task 1: Upgrade the first Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-MG1
Tool	Setup.exe
Location	\LON-DC1\Media\SCOM2012R2

2. Restart LON-MG1
3. Run the System Center 2012 R2 Operations Manager Upgrade wizard to upgrade the Management Server.
4. On the **Configure Operations Manager accounts** page, use the following **Domain Account** credentials:
 - Domain\User Name: **Contoso\svc_SCOM2007_das**
 - Password: **Pa\$\$w0rd**
5. Accept all other default settings.

► Task 2: Upgrade the second Management Server

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
----------	-------

Location	Value
Computer	LON-RMS
Tool	Setup.exe
Location	\LON-DC1\Media\SCOM2012R2

2. Restart LON-RMS.
3. Install ReportViewer.msi.
4. Run the System Center 2012 R2 Operations Manager Upgrade wizard to upgrade the Management Server.
5. On the **Configure Operations Manager accounts** page use the following **Domain Account** credentials:
 - Domain\User Name: **Contoso\svc_SCOM2007_das**
 - Password: **Pa\$\$wOrd**
6. Accept all other default settings.

► Task 3: Verify the success of the upgrade

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	LON-RMS
Tool	Operations Console
Pane	Administration
View	Management Servers

2. Confirm that LON-RMS and LON-MG1 are in a healthy state.
3. Run the **Management Group** report from the Microsoft ODR Report Library, and confirm the report is generated as expected.
4. Close the Operations console.

 **Note:** If either LON-MG1 or LON-RMS appear in a greyed out state in the Operations console, restart LON-RMS and LON-MG1.

Results: After this exercise, you should have upgraded the Management Group to System Center 2012 R2 Operations Manager. You should have also confirmed that the upgrade was successful by verifying that the Management Group is operating as expected.

Question:

When you upgrade Operations Manager 2007 R2 to System Center Operations Manager 2012, what is the first component you should upgrade?

Question:

When you upgrade Operations Manager 2007 R2 to System Center Operations Manager 2012, what are the last components you should upgrade?

Module Review and Takeaways



Best Practice: When you run the Management Group upgrade on the RMS, you are prompted for the System Center Configuration service and System Center Data Access service accounts. It is recommended that a Domain Account be used.



Best Practice: Action accounts can run under a local system account, or be a domain or local user account. In a low-privilege scenario, as a minimum, the following permissions should be assigned to the action account:

- Member of the local Users group
- Member of the local Performance Monitor Users group
- "Allow log on locally" permission (SetInteractiveLogonRight)

Review Question(s)

Question: You must upgrade a System Center 2012 Operations Manager Management Group to System Center 2012 R2 Operations Manager. What must you do before upgrading to System Center 2012 R2 Operations Manager?

Real-world Issues and Scenarios

- Before you upgrade to System Center 2012 R2 Operations Manager, or before you install a new System Center 2012 R2 Operations Manager Management Group, review the Preparing your environment for System Center 2012 R2 Operations Manager section on TechNet here: <http://go.microsoft.com/fwlink/?LinkId=391268>

Known issues when upgrading to System Center 2012 Operations Manager

Following are two common issues that cause an upgrade from Operations Manager 2007 R2 to System Center 2012 Operations Manager to fail.

Upgrade fails when a user role created in Operations Manager does not have an ENU locale

In this scenario, the upgrade fails and the upgrade log reports the following error.

```
Error: :Failed to update user role: : Threw Exception.Type:  
Microsoft.EnterpriseManagement.Common.NullConstraintException, Exception Error  
Code: 0x80131500, Exception.Message: Parameter UserRoleDisplayName cannot be null.
```

You can use the following SQL query against the operational database to determine if any user roles do not have an ENU locale:

```
SELECT  
    DISTINCT UV.UserRoleId AS [UserRoleId],  
    LT.LTVValue AS [RoleName],  
    LT.LanguageCode AS [LanguageCode]  
FROM UserRoleView AS UV WITH(NOLOCK)  
INNER JOIN LocalizedText AS LT WITH(NOLOCK)  
    ON UV.UserRoleId = LT.LTStringId  
WHERE LT.LanguageCode <> 'ENU'
```

If the query returns any user role IDs, the following query can be used to fix them.

```
DELETE LocalizedText  
WHERE LTStringId IN (  
    SELECT DISTINCT LT.LTStringId  
    FROM UserRoleView AS UV WITH(NOLOCK)  
    INNER JOIN LocalizedText AS LT WITH(NOLOCK)
```

```

    ON UV.UserRoleId = LT.LTStringId
    WHERE LT.LanguageCode <> 'ENU'
) AND LanguageCode <> 'ENU'

```

In addition, the following query should be also be executed.

```

SELECT *
FROM LocalizedText
WHERE
    LTValue LIKE '%Operation%Manager Report%' AND
    LTStringId NOT IN (
        SELECT DISTINCT(LTStringId)
        FROM LocalizedText
        WHERE LanguageCode = 'ENU'
    )

```

If any results are displayed, the following query should be executed.

```

UPDATE LocalizedText
SET LanguageCode = 'ENU'
WHERE
    LTValue LIKE '%Operation%Manager Report%' AND
    LanguageCode <> 'ENU' AND
    LTStringId NOT IN (
        SELECT DISTINCT(LTStringId)
        FROM LocalizedText
        WHERE LanguageCode = 'ENU'
    )

```

Upgrade fails when a User Role does not contain a display name

If any user role in Operations Manager does not have a valid display name, the upgrade will fail. To determine if any user roles do not have a valid display name, you can run the following Operations Manager Windows PowerShell cmdlet.

```
Get-UserRole | ft Name, DisplayName
```

If any user roles are returned without a display name, you can use the Operations console to correct them.

Module 4

Configuring Fabric and Application Monitoring

Contents:

Module Overview	4-1
Lesson 1: Introduction to Management Packs	4-2
Lesson 2: Configuring Application Monitoring	4-17
Lesson 3: Configuring Network Device Monitoring	4-30
Lesson 4: Configuring Fabric Monitoring	4-36
Lab: Configuring Application and Fabric Monitoring	4-47
Module Review and Takeaways	4-65

Module Overview

After you deploy Microsoft System Center 2012 R2 Operations Manager and install agents on the computers hosting the applications and services you need to monitor, you need to install Management Packs to start monitoring them. Before you install Management Packs, you need to understand Management Pack concepts, including all the elements of a Management Pack.

You should also understand how to configure fabric and application monitoring in Operations Manager for both your private and public cloud environments, including how Operations Manager and System Center 2012 Virtual Machine Manager is integrated and how you integrate Operations Manager with Microsoft Azure.

Knowing how to configure Management Packs to monitor applications that are running on your fabric, such as Microsoft SQL Server, Microsoft Internet Information Services (IIS) Server, and Microsoft SharePoint Server, is also important. Finally, you should understand how to configure integration between Operations Manager and System Center Advisor so that you can view Advisor alerts relating to your fabric components and applications.

Objectives

After completing this module, students will be able to:

- Describe Management Pack fundamentals in Operations Manager.
- Configure Network Device Monitoring in Operations Manager.
- Configure fabric monitoring in Operations Manager.
- Configure application monitoring in Operations Manager.

Lesson 1

Introduction to Management Packs

Management Packs provide core functionality to an Operations Manager Management Group. In addition to storing the rules and monitors for the objects they are designed to monitor, Management Packs also include the views that are used in the Monitoring pane of the Operations console and the Web console for monitoring alerts, events, and performance data. Management Packs also include a number of other elements such as object discoveries, tasks, overrides, and knowledge to assist with troubleshooting alerts, if generated.

You need to understand how Management Packs work in Operations Manager and how to customize the monitored environment by creating new rules, monitors, and overrides, including how to target each of these correctly.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe the most commonly used Management Packs.
- Import Management Packs.
- Describe sealed versus unsealed Management Packs.
- Create Management Packs.
- Describe Management Pack elements, including:
 - Object discoveries
 - Rules
 - Monitors
 - Targeting
 - Run As accounts and Run As profiles
 - Overrides
 - Diagnostic and recovery tasks
 - Agent and console tasks

Most Common Management Packs

Depending on your environment and the types of servers and applications that require monitoring, Operations Manager contains several standard Management Packs that you can deploy to enable base monitoring of your infrastructure. Typically, you would deploy Management Packs for the following products and technologies:

- Active Directory Domain Services (AD DS)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Common Management Packs include:

- Active Directory Domain Services (AD DS)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Windows Server Base Operating System
 - Windows Server 2008
 - Windows Server 2012
- Windows Print Server



- Windows Server based operating system
 - Windows Server 2008
 - Windows Server 2012
- Windows Print Server

If you also use Microsoft products such as SharePoint and Exchange, you should include Management Packs for the following products:

- IIS Server
- SQL Server
- SharePoint Server
- Microsoft Exchange Server

You can download these Management Packs at no cost from the Management Pack catalog website:



Microsoft System Center Marketplace

<http://go.microsoft.com/fwlink/?LinkId=391269>

You can download the Management Packs and their associated guide documents. You can also find details of third-party management packs from the Management Pack catalog website. However, be aware that the main purpose of each Management Pack is to monitor, report, or alert about particular issues that might be occurring with the application or component for which it was designed. Therefore, if you import all the Management Packs in the preceding list at one time, without applying any overrides or customization to them, you might find that the Operations Manager console starts to fill with alerts within a short time. A best practice is to install one or only a small number of Management Packs at one time and then wait a minimum of 24 hours. During this time, you should monitor the alerts that are generated. This enables you to fine-tune the Management Pack with overrides that are customized for your environment before you install additional Management Packs.

Rules and monitors within each Management Pack have default threshold values assigned to them. Usually, these values are sufficient. However, in some instances, you might need to adjust these values to meet specific monitoring requirements in your environment. For example, suppose you have a page file that is located on drive P on all production servers. This page file is typically sized for the exact size of the disk, and Operations Manager generates an alert to notify you that available disk space is low on these drives. However, you can create a group that contains all logical disks that have a display name of P, and then apply an override to the group that disables the logical disk space monitor for these logical disks. Overrides are covered in more detail later in this lesson.

Be aware that most Management Packs from Microsoft are sealed (meaning they are read-only). Creating a new Management Pack to store any overrides that must be applied to a sealed Management Pack is recommended. Creating Management Packs is covered in detail in Module 9, "Management Pack Authoring."

The Process of Importing Management Packs

As described earlier in this module, Management Packs can be obtained from a number of different sources, such as the Management Pack catalog website or third-party vendors. To use these Management Packs, you must import them into Operations Manager. You can use the Operations console to download and import Management Packs, or you can download them separately from the Management Pack catalog website or any other source, and then import them later.

To import Management Packs, in the Administration pane of the Operations console, in the Tasks pane, you use the Import Management Packs task that is available when the Management Packs node is selected. This opens the Import Management Packs wizard, which provides two methods for importing Management Packs:

- **Add from disk.** When you click the Add From Disk option, you can browse either a local disk or a network share where the Management Packs have been downloaded. This option is typically used when the Operations Manager server does not have access to the Internet and thus cannot download the Management Packs directly from the Management Pack catalog website. This option is also used for specific Management Packs that cannot be imported directly from the Management Packs catalog, such as the Exchange 2010 Management Pack or the Management Pack for SQL Server.
- **Add from catalog.** When you click the Add From Catalog option, you are connected to the Management Pack Catalog Web Service, where all online Management Packs are available for downloading and importing. By default, all Management Packs are listed, but you can modify the list to display only updated Management Packs for those Management Packs you have already imported. This is useful for quickly determining if any updated Management Packs are available for your environment. You can also display Management Packs that have been released within the last three or six months, and search for specific Management Packs by using the Find option.

Management Packs you select to import are displayed in the Import Management Packs wizard, where you can view details such as the Name, Version, Release Date, and any License Terms. Also provided in the wizard are a Status column and Status Details window that you can use to troubleshoot any incompatibility issues with Management Packs. For example, many Management Packs depend on other Management Packs, and unless those Management Packs are installed first, dependent Management Packs cannot be installed. In this scenario, an Error status is displayed next to the Management Pack, and the Status Details window provides details relating to why this Management Pack cannot be installed. You can also click the Error link that appears next to the Management Pack, which will open an Import Management Pack Error window displaying the Management Packs that must be installed first.

Some Management Packs contain Write actions that might pose a security risk to the Operations Manager environment. For this reason, whenever a Management Pack containing one or more Write actions is to be imported, a Security risk status is displayed in the Status column of the Import Management Packs wizard. This risk status is useful when you have selected a number of Management Packs to import, because you can quickly determine which ones contain Write actions and confirm that you want to install them. If you do not want to install them, you can right-click the Management Pack and then click Remove to remove it from the list.

After adding the Management Packs you want to import into the Import Management Packs wizard, you click Install to install them. During the installation process, view the Status column to determine when each Management Pack is imported.

You can download Management Packs from System Center Marketplace

You can import Management Packs by using the Import Management Packs wizard

Using the Import Management Packs wizard, you can:

- Import Management Packs from a local disk or network share
- Import Management Packs from the Management Pack catalog website

After the Management Packs are installed, they are listed in the Management Packs node in the Administration pane of the Operations console.

You can also use the Download Management Packs task to download Management Packs from the Management Pack catalog. This is useful if you want to download Management Packs and make them available to multiple Operations Manager environments such as development and production.

 **Note:** You can also use the Import-SComManagementPack PowerShell Cmdlet to import management packs into Operations Manager. The following example imports a management pack named DinnerNow:

```
Import-SComManagementPack -Fullname "C:\Mps\DiinnerNow.xml"
```

Sealed vs Unsealed Management Packs

Management Packs can either be *sealed* (read-only) or *unsealed* (read/write). You can easily determine whether a Management Pack is sealed or unsealed by looking at the file name extension. A sealed Management Pack has an extension of .mp or .mpb, whereas an unsealed Management Pack has an extension of .xml.

Note that an .mpb file is a Management Pack bundle that contains multiple Management Packs, and optionally other files such as images or code, which are to be deployed to agents in Operations Manager after the Management Packs have been deployed.

A sealed Management Pack provides a number of unique characteristics that an unsealed Management Pack does not, as described in the following sections.

Read-Only

A sealed Management Pack cannot be written to. If changes must be made to the Management Pack, those changes must be done in the unsealed XML version first. Then a new sealed Management Pack can be created from the updated XML Management Pack.

Enforced Version Control

When an updated sealed Management Pack is imported, version control is enforced to help ensure backward compatibility. When an updated unsealed Management Pack is imported, the new version is always installed regardless of whether backward compatibility is maintained.

Management Pack Referencing

Certain Management Packs can share elements such as classes, groups, or modules with other Management Packs, and these are typically known as *library Management Packs*. Library Management Packs are then referenced by other Management Packs, making them a dependent Management Pack. Only sealed Management Packs can be referenced by other Management Packs.

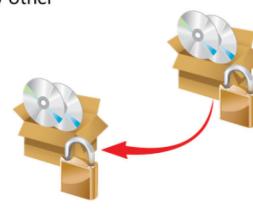
You do not need to seal Management Packs before importing them into Operations Manager, but there are certain scenarios in which a Management Pack must be sealed. These include:

Sealed Management Packs have the following characteristics:

- Are read-only
- Enforce version control
- Can be referenced by other Management Packs

Windows Server Operating System Library Management Pack

SQL Server 2012 Management Pack

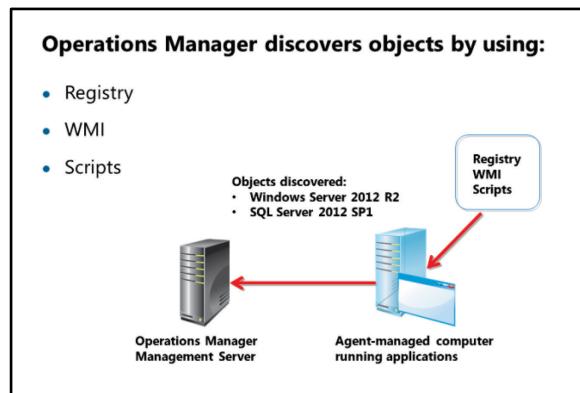


- **The Management Pack is to be referenced by other Management Packs.** If you are creating a library Management Pack to share common elements such as classes or groups, you must seal the Management Pack before it can be referenced.
- **The Management Pack has been developed for an external source.** If you have developed a Management Pack for an external source such as a customer, the Management Pack should be sealed to ensure the contents cannot be modified. Doing so also forces the customer to make changes by using an Overrides Management Pack, ensuring that any updates to the sealed Management Pack do not affect the customer's environment.
- **The Management Pack has been developed for multiple business units.** If the Management Pack is to be used by multiple business units within an organization, the Management Pack should be sealed to ensure each business unit saves any customizations in their own overrides Management Pack.

When sealing a Management Pack, you use a certificate to secure its contents. Sealing Management Packs is covered in detail later in Module 9 "Management Pack Authoring".

Object Discoveries

Before you can perform any monitoring or reporting of an application in Operations Manager, you should import the relevant Management Pack. This enables Operations Manager to discover the instances of the application in the environment, and then apply monitoring that is based on the Management Pack's default settings. For example, when you import the Active Directory Management Pack, a set of classes, discoveries, rules, monitors, views, tasks, and reports are imported. Operations Managers uses this information to determine how AD DS operates, the components that it contains, and how it should be monitored appropriately.



Object discoveries in Operations Manager are used to discover the application or components that the Management Pack will monitor.

An *object* in Operations Manager is the basic unit of management, which includes computers, logical disks, and databases. Objects can also represent an application such as SQL Server. Object discoveries are included with Management Packs and run on an agent-managed computer to determine which objects should be created in Operations Manager and what associated values should be applied to them.

So that new objects can be discovered automatically, object discoveries are typically run on a schedule. For example, the Windows Server Network Adapter Discovery Rule runs one time per day. This means that any new network adapters are discovered within 24 hours. Objects are also updated based on object discoveries. Therefore, if an object is removed from the agent-managed computer, it is also removed from Operations Manager.

Object discoveries can use several different methods to discover objects on a managed computer. These methods include the following:

- **Registry.** The registry is the preferred method of object discovery in Operations Manager. It has the least overhead as measured by processor and memory usage on the agent-managed computer. Most Windows-based applications use the registry to store information that relates to the application that is installed. This includes the application version, the update level, installation directory, and other

application-specific data. Object discoveries can use information that is obtained from registry keys and values to determine whether an application is installed on the managed computer. After discovery, relevant Management Packs, including their rules and monitors for the specific version of the application, are downloaded to the agent so that monitoring can start.

- **WMI (Windows Management Instrumentation).** WMI stores information that relates to the computer and the operating system that is running. Object discoveries can use WMI to query its database for any information that is held. If an installed application also has a WMI provider, this application can also be queried by using an object discovery.
- **Scripts.** If the object discovery requires information that cannot be obtained by either the registry or WMI methods, you can create a discovery script to obtain the relevant information to discover the object. Scripts are typically written by using Microsoft Visual Basic for Applications (VBScript) or JScript by default, or Windows PowerShell.

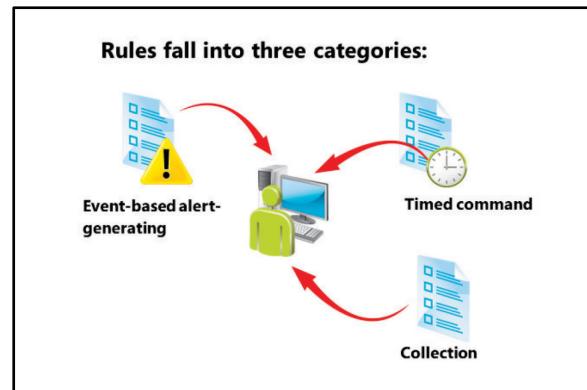
Rules

Management Pack rules provide three functions in Operations Manager. The following sections provide a detailed description of each type of rule.

Alert-Generating Rules

Alert-generating rules provide a method of generating alerts that are based on the occurrence of a given event, such as an event in the system event log or a text string in an application log file.

The following table describes event-based alert-generating rules provided in Operations Manager.



Event-based alert-generating rule	Description
Generic CSV Text Log	If an application writes its log information to a comma-separated values file (CSV), you can use this rule to generate alert-based parameters and values that are detected in the log file.
Generic Text Log	Similar to the Generic CSV Text Log, this rule can be used to detect parameter values in a generic text log and then generate an alert based on detected values.
NT Event Log	<ul style="list-style-type: none"> The NT Event Log rule generates alerts that are based on events in the Windows Event Log, including: <ul style="list-style-type: none"> Application Hardware Microsoft Internet Explorer Key Management Service Operations Manager System
SNMP Trap	The SNMP Trap rule is used to target objects, such as a Simple Network Management Protocol (SNMP) network device. The rule

Event-based alert-generating rule	Description
	then generates an alert based on the object identifier (OID).
Syslog	<i>Syslogs</i> are log files that are typically used by UNIX-based and Linux-based operating systems. Network devices such as routers and firewalls can also use syslogs. The Syslog rule can generate an alert based on detected parameters and values, such as Warning or Intrusion.
Unix/Linux Shell Command	Using a Run As Profile, you can use this rule to run a binary or script file or a single-line shell command against a Linux or UNIX computer. An alert is generated based on a configured expression that is applied to the output.
WMI Event	The WMI Event rule generates an alert based on a WMI event by querying a WMI namespace.



Note: Alert-generating rules in Operations Manager do not affect the health state of an object. Only monitors can affect the health state of an object.

Collection Rules

Use *collection rules* in Operations Manager to collect and store data to use in views and reports. For example, you might require an event view that displays computers that have logged a specific event, such as a backup failure. You can create an NT Event Log collection rule that detects the event ID in the Application Event Log and then target it at the Windows Computer class. The Operations Manager agent detects when the event is generated and stores the details in the Operations Manager database. You can then create the event view based on the Event ID or other criteria, such as the computer that logged the event. Other collection rules are available for SNMP, text and CSV logs, WMI, and Syslogs.

You can also create performance-based collection rules for SNMP, WMI, and Windows Performance counters. These rules are useful in creating capacity-planning reports or performance views. When you create a Windows Performance collection rule, you can select the performance object, counter, and instance from a remote computer. This makes identifying and selecting the counter much faster and easier. You can also enable optimization and either increase or decrease the accuracy by storing more or fewer data points, respectively, in the database.

You can create probe-based collection rules to collect data based on scripts or UNIX/Linux shell commands.

Timed Command Rules

You can use *timed command rules* to run commands, batch files, executables, or scripts on a scheduled basis. This is useful when you are running repetitive tasks such as clearing log files, or performing maintenance tasks such as backing up a database. You can create two types of timed command rules: execute a command, and execute a script.

For each rule you specify the target, such as Windows Server, and then configure the schedule. The schedule can be configured to run every x seconds, minutes, hours, or days. You can create a schedule that is based on a fixed weekly basis. This can include specified days of the week or can span multiple days between start and end dates and times. Then you add the path to the command or scripts such as c:\windows\system32\ping.exe, and add any required parameters that should be passed to it.

Monitors

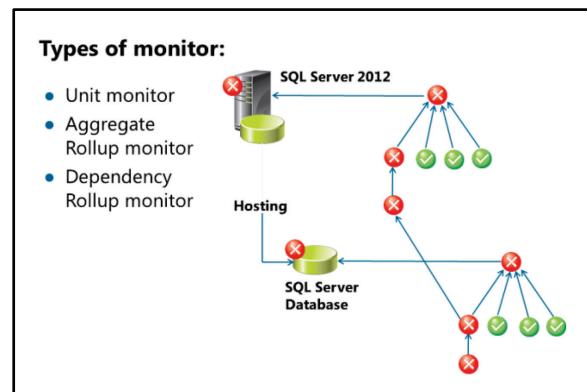
Use monitors in Operations Manager to show the health state of an application or object.

Depending on the monitor type, the health state of a monitored object can be either of the following:

- Two State (green or red)
- Three State (green, yellow, or red)

You can view these states from different views in the Operations console. You can use these states to instantly see an application or object's overall health state. The following describes how a monitor calculates an object's health state:

- If the available disk space on a disk drive falls lower than 10 percent, the health state is red. In addition to the red state that is displayed in the Operations console, an alert could also be generated.
- If the available disk space on a disk drive falls lower than 15 percent, the health state is yellow. An associated alert could also be generated. You can use this alert to warn an operator of a pending disk space issue.
- If the available disk space on a disk drive is greater than 15 percent, the health state is green. This indicates a healthy state.



Both rules and monitors collect monitoring data, but monitors do not store any collected monitoring data in the Operations Manager databases. Monitors only store health state changes and alert information in the Operations Manager databases.

Following are three types of monitors in Operations Manager:

- Unit monitors
- Aggregate rollup monitors
- Dependency rollup monitors

Unit Monitor

Use unit monitors to monitor specific counters, events, scripts, and services. This monitor can also generate alerts.

Aggregate Rollup Monitor

Use aggregate rollup monitors to show the health state of other monitors that are targeted at an object. You can use the following monitors with aggregate rollup monitors:

- Unit monitors
- Dependency rollup monitors
- Other aggregate rollup monitors

For example, you can use an aggregate rollup monitor to group multiple monitors into a single monitor that then can be used to depict an overall health state.

For every target in Operations Manager, there are four top-level aggregate rollup monitors:

- Availability
- Configuration

- Performance
- Security

Use these aggregate rollup monitors to group similar monitors that show an object's health state.

Dependency Rollup Monitor

Use dependency rollup monitors to roll up health states for objects that are linked by a containment or hosting relationship. These relationships are defined in most Management Packs. You can use them to make the health state of an object dependent on the health state of components that are contained or hosted.

Use dependency rollup monitors in Operations Manager to indicate that the overall state of an object should change if a given percentage of an object's health state changes.

The following slide shows how a dependency rollup monitor operates. The slide displays a hosting relationship between SQL Server 2012 and the SQL Server databases. Although both objects have monitors associated with them, the relationship between them enables the health state to be rolled up.

For example, if the SQL Server database becomes unavailable, its health state turns red. This converts the overall health state for SQL Server 2012 to red. This is shown on the slide.

For more information about monitors and rules in Operations Manager visit the following website.



Monitors and Rules

<http://go.microsoft.com/fwlink/?LinkId=404084>

Targeting

Targeting is an important concept in Operations Manager that must be understood before customizing the monitored environment with rules, monitors, or overrides. When a rule or monitor is created in Operations Manager, you must select a target. The *target* determines the following characteristics of the associated rule or monitor:

- Where the rule or monitor will be run
- How many copies of the rule or monitor will run on the agent
- What object the data will be associated with
- What properties will be available for the alert description and expression

The target determines the following for rules and monitors:

1. Where the rule or monitor will be run
2. How many copies of the rule or monitor will run on the agent
3. What object the data will be associated with
4. What properties will be available for the alert description and expression



You must understand how targeting works in Operations Manager so that rules and monitors you create are targeted appropriately.

When you select a target in Operations Manager, you select a class of object rather than a specific instance of an object, such as the Windows Server class, not a specific server. A *class* is the definition of an object. You can think of every object in Operations Manager as an individual instance of a class.

You can view the individual instances of any class by using the Discovered Inventory view in the Monitoring pane of the Operations console. To do this, follow these steps:

1. In the Operations console, click the **Monitoring** pane, and then click **Discovered Inventory**.

2. In the **Tasks** pane, click **Change Target Type**.
3. In the **Select Items to Target** window that opens, in the **Look for** box, type **Windows Server 2012 Logical Disk**.
4. Select the **Windows Server 2012 Logical Disk** target, and then click **OK**.

The Results pane now shows the class, discovered objects of the class, and the properties of the selected object as follows:

- **Class.** Windows Server 2012 Logical Disk
- **Object.** C:
- **Properties.** Windows Server 2012 Logical Disk Properties of C:

The Path column displays the name of the computer on which the object resides.

Every class in Operations Manager has a base class. Think of a *base class* as a group class that contains other related classes. For example, the base class named Windows Operating System contains both the Windows Client Operating System and the Windows Server Operating System classes.

This is important to know when you target your monitor or rule. If you target the Operating System class, for example, the rule or monitor will run on both Windows Server and Windows-based client operating systems.

In System Center Operations Manager 2005 and earlier versions, rules and monitors were targeted at computer groups. A *group* in System Center Operations Manager 2007, Operations Manager 2007 R2 and all versions of System Center 2012 Operations Manager is a collection of objects that can include instances of the same class or different classes.

If you must target a rule or monitor at a single server or group of servers instead of at a class, you should use the following method:

1. Create a group that contains the computer on which the rule or monitor will run.
2. Create the rule or monitor, and then use Windows Computer as the target.
3. Disable the rule or monitor that was just created.
4. Create an override that enables the rule or monitor for the group that was created in step 1.

In addition to scoping overrides, groups can be used to scope views and user roles in the Operations console.



Note: Overrides are covered in detail later in this lesson.

More information about selecting a target can be found at the following link:



Selecting a target

<http://go.microsoft.com/fwlink/?LinkId=321857>

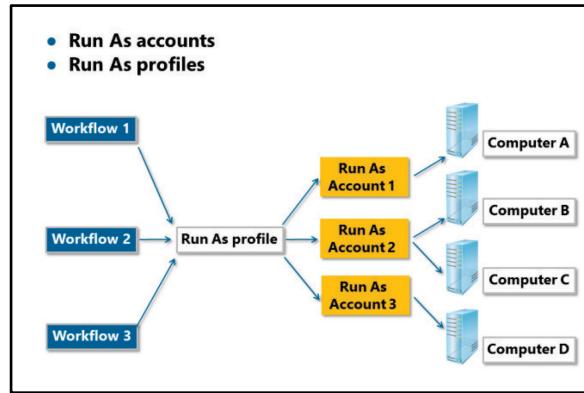
Run As Accounts and Run As Profiles

Rules, tasks, monitors, and discoveries that are defined in a Management Pack require credentials to run on a targeted computer. By default, rules, tasks, monitors, and discoveries run by using the default action account for the agent. For example, if an action is performed on an agent, the credentials that are used for the action come from the agent action account. Frequently, this account might be a local system account.

Run As accounts and Run As profiles let you run different rules, tasks, monitors, or discoveries under different credentials on different computers.

Management Packs no longer share the same identity. Therefore, you can use a low-privilege account as your action account. Run As accounts support the following account types:

- **Windows.** Windows credentials, for example, *domain\user name*, or *user name@FullyQualifiedDomainName*, and the associated password
- **Community String.** SNMP 2 community string
- **Basic Authentication.** Standard basic web authentication
- **Simple Authentication.** A generic user name and password, such as a *webpage*
- **Digest Authentication.** Standard digest web authentication
- **Binary Authentication.** User-defined authentication
- **Action account.** Windows credential that can be assigned only to the action account profile
- **SNMP v3 account.** Used for discovery and monitoring of SNMP v3 network devices



To help you understand how Run As accounts and Run As profiles work, consider the example on the slide. There are three workflows that use the same Run As profile. (*Workflows* contain rules, tasks, monitors, and discoveries.) The Run As profile has three Run As accounts that are associated with it. When the workflow runs on Computer A, it uses the credentials as defined in Run As account 1. When the workflow runs on Computer B and Computer C, it uses the credentials as defined in Run As account 2. When the workflow runs on Computer D, it uses the credentials as defined in Run As account 3.

Operations Manager includes several built-in Run As profiles, including the Active Directory Based Agent Assignment account profile that is used to publish agent assignment settings to AD DS. Other Run As profiles include SQL Server Discovery account and SQL Server Monitoring account. These Run As profiles are typically used in environments where different accounts are required to discover and monitor specific SQL Server instances because of security constraints contained within them.

Run As Account Distribution and Targeting

When you create a Run As profile in Operations Manager, you must configure the Run As accounts and distribution to identify which Run As account credentials will be used and to which computers the credentials should be distributed. In addition, you must also specify the target, such as the group, class, or object, to identify which Run As account will be used to run tasks, discoveries, rules, and monitors on the target.

As part of the Run As profile, you can decide to distribute the Run As account credentials to all agent-managed computers or to only selected computers. This enables you to distribute Run As account information to agent-managed computers more securely, because you can target only the specific computers that require this information.

Suppose you have a computer that is running two instances of SQL Server. For Operations Manager to perform its monitoring, each instance requires a different set of credentials. You can create two Run As accounts that have the relevant credentials for each instance of SQL server. Then you can configure the SQL Server profile with both Run As accounts, and associate each account with each instance of SQL Server. Finally, you can configure the distribution such that both Run As account credentials are distributed to the server running SQL.

For example, if multiple computers hosting SQL Server require different credentials, you can add a Run As account for each credential. Then you can configure the distribution so that the Run As accounts are distributed to the relevant instances of SQL Server.

Overrides

A Management Pack in Operations Manager starts monitoring as soon as it is downloaded and initialized on to an agent. The Management Pack contains elements, such as rules and monitors that are predefined with default thresholds.

The vendor of the Management Pack sets these defaults. These thresholds are used as a definition of a healthy state for the application for which the Management Pack was designed.

When administrators must change the default threshold of a monitored object, they can create an *override* to customize the rule or monitor for their environment.

Administrators can view which overrides affect a managed object by viewing the override summary of the object. You can view this in the Summary node of the Overrides menu.

 **Note:** A user must have at least Advanced Operator rights to create and edit overrides.

You can access the overrides UI by clicking the Overrides toolbar button in different views in the Monitoring and Authoring panes. Wherever the view context defines a single monitor or rule, there is a shortcut option to disable the monitor or rule with an override.

One of the key concepts with overrides is target context. *Target context* refers to the scope where the override-modified monitor or rule will be deployed. An *override target* must be an object (instance), a group, or a class. Class-targeted overrides are available only to authors and administrators.

The Override Properties dialog box is used to display the properties of a custom override. A *custom override* changes one or more parameters of a single monitor or rule, and has a target context. You can also use this dialog box to create a new custom override. In that case, none of the check boxes in the Override column are initially selected.

When you create an override, the Overrides dialog box cannot access the information that is provided in the Monitor/Rule Properties dialog box. It only recognizes the list of override-controlled parameters that are available. For example, although threshold is an override-controlled parameter for a monitor, the name of the performance counter that the threshold is specified for is not an override-controlled parameter. Therefore, the Overrides dialog box cannot recognize or list the counter name for the threshold value. This can make it challenging to know how to set the override.

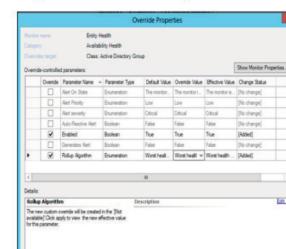
Each Management Pack has default settings and thresholds

Overrides are used to change these settings and thresholds

Overrides can target:

- Object (instance)
- Group
- Class

User must have at least Advanced Operator rights to create overrides



The workaround is for the Overrides dialog box to invoke the monitor or rule properties dialog box (as read-only, even for administrators) so that the user can examine it and then determine how the overrides are set in relation to the actual monitor configuration.

The Overrides Summary option provides a list of all overrides that are configured for a particular instance or category.

More information about How to Override a Rule or Monitor can be found at the following link:

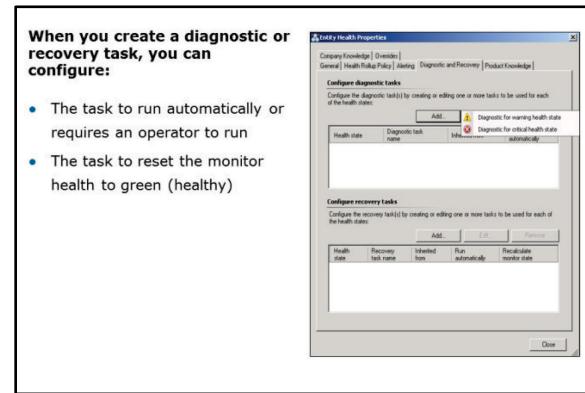
How to Override a Rule or Monitor

<http://go.microsoft.com/fwlink/?LinkId=321858>

Diagnostics and Recovery Tasks

When Operations Manager detects an issue in the environment by using a monitor, its health state changes to either a warning or a critical state. Each monitor can include information that relates to the cause of the issue, which is useful in diagnosing and recovering from the detected issue. You can add a diagnostic or recovery action to a monitor by viewing its properties.

When adding a diagnostic or recovery task to a monitor, you can configure the task to run automatically, or configure it to require operator intervention.



In addition, when you add a recovery task to a monitor, you can enable the monitor to run on demand. This can be useful when you need to recalculate the health state of the monitor.

Depending on the type of diagnostic or recovery task, you might decide to automate the action and provide automatic remediation of an issue that is detected by the associated monitor. For example, a monitor can be configured by using a recovery task that removes temporary files when it detects available disk space is at a critical level.

More information about diagnostic and recovery tasks can be found at the following link.

Diagnostic and Recovery Tasks

<http://go.microsoft.com/fwlink/?LinkId=321859>

Agent and Console Tasks

Tasks are created in the Tasks view under the Management Pack Objects node in the Authoring pane of the Operations console. In the Tasks pane, use the Create A New Task option to open the Create Task Wizard, which guides you through the configuration of the task.

There are two types of tasks that you can use with Operations Manager:

- Agent task
- Console task

Two types of tasks can be used with Operations Manager:

Agent task



Agent-managed computer

Console task



Operations Manager Console

Agent Task

Agent tasks run on the managed computer or agent. By default, they run under the security context of the default action account of the agent. A typical agent task runs a script that collects data from a computer that is hosting the agent, such as a log file. Agent tasks can be created by using one of the following three task types:

- **Command Line.** The Command Line task allows you to specify the path to the command line file to use. You can include any relevant parameters that should be used with the command. This is useful because you can include variables that Operations Manager uses, such as IP Address or DNS Display Name.
- **UNIX/Linux Shell Command.** The UNIX/Linux Shell Command task is used to run either a binary or script file, or a single-line shell command. With this task, you must also specify a Run As profile that will be used to supply the credentials on the computer that is running UNIX/Linux where the task will run.
- **Script.** The Script task is used to run a script against a targeted computer. You include the script name, and then either manually enter or paste the script into the Create Task Wizard. You can also add parameters that can be included in the script such as DNS Domain Name or Display Name. This task can be very useful because you can use context-sensitive parameters, such as the Computer Name of the selected agent, in the Operations console.

Console Task

Console tasks run on the same computer that hosts the Operations console. A typical console task uses Remote Desktop to connect to a selected computer. Console tasks run under the security context of the user who is running the Operations console. Console tasks can be created by using one of the following three task types:

- **Alert Command Line.** The Alert Command Line task is used to run a command line or batch file based on an alert. The task then becomes available in the Tasks pane when the alert is selected. This can be useful when you need to forward an alert to an external source such as a ticketing system. When configuring the task, you supply the path to the application to run and can optionally include parameters such as the Severity and Resolution State.
- **Command Line.** The Command Line task is used to execute a command-line application or batch file based on a selected class. When the class is selected in the Operations console, the task becomes available in the Tasks pane. When configuring the task, you specify the Task Target such as Agent or Computer. You then specify the full path and name of the application to run, and optionally include parameters such as Display Name or Principal Name.

- **Event Command Line.** The Event Command Line task is used to execute a command-line application or batch file based on an event. When the event is selected in the Operations console, the task becomes available in the Tasks pane. When configuring the task, you specify the full path and name of the application to run, and optionally include parameters such as Logging Computer or ID.

More information about Console tasks and Agent tasks can be found at the following link.



Tasks

<http://go.microsoft.com/fwlink/?LinkId=321860>

Demonstration: Viewing Management Pack Objects by using the Operations Console

In this demonstration you will learn how to view Management Pack objects by using the Operations Console.

Demonstration Steps

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Authoring
View	Management Pack Objects

2. Review the **Management Pack Objects** in the following nodes:

1. Attributes
2. Monitors
3. Object Discoveries
4. Rules
5. Tasks
6. Views

Question: What are the three methods that a discovery in an Operations Manager Management Pack can use to discover an application?

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
Rules can affect the health state of a monitored object.	

Lesson 2

Configuring Application Monitoring

As part of your monitoring requirements, a number of applications will need to be monitored. This includes Microsoft applications such as SQL Server, IIS Server, and Microsoft SharePoint Server. Because these Management Packs monitor components that are present in multiple applications, it's important that you learn the most common configuration steps for each of these management packs.

For example, your instance of SQL Server might have a security constraint in which each database requires separate logon credentials. In this scenario, you must understand how Run As accounts and Run As profiles can be used to ensure the correct credentials are distributed and used for each database.

Lesson Objectives

After completing this lesson, students will be able to:

- Configure monitoring for the base operating system.
- Configure monitoring for SQL Server.
- Configure monitoring for IIS Server.
- Configure monitoring for SharePoint Server.

The Process of Configuring Base Operating System Monitoring

The System Center Management Pack for Windows Server Operating System will be one of the first (if not the first) Management Pack that you deploy in your Operations Manager Management Group. Not only is it required to monitor the base operating system, but it is also required by other Management Packs such as the IIS Management Pack as a dependency. As mentioned earlier, Management Packs can reference other Management Packs. The IIS Management Pack references the Windows Server Library and Windows Server 2012 Discovery

Management Packs that are installed when you install the System Center Management Pack for Windows Server Operating System. Similar dependencies exist for other Management Packs, such as the Windows Server DHCP 2012 R2 Management Pack.

It is important to obtain the most up-to-date version of a Management Pack to ensure you benefit from any new or updated monitoring capabilities and any updated versions of the application it supports. For this reason, using the Add From Catalog option is recommended when installing Management Packs, because this option enables you to connect to the Management Pack catalog website and obtain the most current Management Pack versions available.

For the Windows Server operating system, a new Management Pack 6.0.7061.0 was released with the release of System Center 2012 R2 Operations Manager. With each Management Pack, a Management Pack guide is also provided. Reading the guide before installing a Management Pack is recommended to ensure you understand required prerequisites and any necessary configuration for the Management Pack to perform its monitoring functions.

The System Center Management Pack for Windows Server Operating System includes:

- Performance monitoring
- Availability monitoring
- Health state monitoring
- Reports
- Tasks



The System Center Management Pack for Windows Server Operating System does not require any additional configuration after you install it. However, you might need to perform additional tasks depending on your monitoring requirement and security constraints. Additional task could include:

- **Overriding default thresholds.** All Management Packs have default (best practice) thresholds configured to provide default monitoring based on a typical installation of the application it was designed for. You might need to override particular thresholds to customize monitoring for your environment. For example, you might need to reduce the disk space availability monitor for a server that is known to be low on disk space during a backup process. When creating overrides, it is recommended that you create an override Management Pack that will be used to store the overrides for each application or component. This not only provides an easy method of backing up customizations made to a Management Pack, but it also allows for customizations to be exported and used in other Operations Manager environments.
- **Enabling additional discoveries, monitors, and rules.** Not all monitors and rules are enabled by default in some Management Packs. For example, by default, in the System Center Management Pack for Windows Server Operating System, physical disk partitions are not discovered. Only logical disks are discovered. If you want to monitor physical disk partitions, you must enable the Object Discovery for it. The Management Pack guide included with the Management Pack will include details of additional monitoring that can be enabled, if appropriate.
- **Monitoring in low-privilege scenarios.** As a result of security constraints, you might need to configure a low-privileged account for use with the Management Pack. By default, the System Center Management Pack for Windows Server Operating System uses the agent action account to run rules, monitors, and object discoveries. When the agent action account is running as a Local System account, all required permissions are satisfied. If you need to use a low-privileged account instead of a Local System account, the account used must have at least the following permissions:
 - Member of the local users group
 - Member of the local Performance Monitor Users group
 - Granted Log On Locally rights

Two discoveries and one monitor, however, must use a high-privileged account. These are:

- Mount Point Discovery
- Physical Disk Discovery
- Monitoring the Computer Browser service

By default, these discoveries and monitor have already been configured to use the Privileged Monitoring Account Run As profile, which uses the Local System account, so no further configuration is required.

Monitoring the Windows Server Operating System

After installing the System Center Management Pack for Windows Server Operating System, Operations Manager starts to discover and monitor the operating system on agent-managed computers. In the Monitoring pane, in the Microsoft Windows Server folder, you can use a number of views to determine the health, performance, and availability of Windows-based servers in your environment. Some of the most common and useful views are described in the following table.

Microsoft Windows Server view	Description
Windows Server State	The Windows Server State view displays the health state for every monitored Windows-based server in the environment. This includes any server hosting an Operations Manager feature such as Management Servers. You can use this view to quickly become aware of any servers that are in a warning (yellow) or critical (red) health state. Many properties of the selected server are also displayed in the Detail View. Properties include DNS Name, IP Address, Domain Name, Active Directory Site, and the number of Physical and Logical Processors. By right-clicking a server here, you can also open other context-sensitive views, such as the Health Explorer, Event View, and Performance View.
Health Monitoring	A number of health state views are available in the Health Monitoring folder. These include Cluster Disks Health, Cluster Shared Volumes Health, Disk Health, Network Adapter Health, and Operating System Health. These views are useful when troubleshooting an unhealthy server, because you can check the health state of each component and correlate it with any events or alerts that have been generated.
Operating System Events	<p>The Operating System Events folder provides event monitoring views for the following events:</p> <ul style="list-style-type: none"> • Failed Software Update Installations • Services or Drivers Failing to Start • Shares with Invalid Configuration • Unexpected Service Termination <p>These views display any events of this type detected on monitored servers and allow you to view the event details, such as the logging computer that generated them.</p>
Performance	<p>A number of performance views are available in the Performance folder, including:</p> <ul style="list-style-type: none"> • Disk Capacity • Disk Utilization • Memory Utilization • Processor Performance <p>These views are useful when troubleshooting performance problems with a server because they can provide both an up-to-date status and a historical view of how a server has performed over a given time period.</p>

Windows Server Reports

Many reports are made available after you install the System Center Management Pack for Windows Server Operating System, including the following:

- Memory Performance History
- Operating System Configuration
- Operating System Performance

- Paging File Performance History
- Physical Disk Performance
- Performance History (Processor Queue Length)
- Performance History (Percent Processor Time)

Use these reports to obtain a historical view of a server's performance and availability. They also help with capacity planning.

Note that typically, after installing the Windows System Center Management Pack for Windows Server Operating System, Management Packs for applications such as DNS, DHCP, and AD DS are installed. This ensures the key functions in a Windows Active Directory domain are monitored.

Windows Computer Tasks

When a Windows-based computer is selected in a state view such as the Windows Server State view, useful tasks become available in the Tasks pane. Select these tasks to perform a specific action on the selected computer. Some of the most useful tasks are:

- Computer Management
- Display Account Settings
- Display Server Statistics
- Ping Computer
- Remote Desktop
- Route Print

Tasks provide useful troubleshooting help and also reduce troubleshooting time, because you can perform most of them from within the Operations console and do not need to log on to the server. When running a task, you can choose to use the preferred Run As account or, if required, you can manually specify the credentials to use when the task is performed.

System Center Management Pack for Windows Server Cluster

Although the System Center Management Pack for Windows Server Cluster is a separate Management Pack, you should note that Operations Manager also supports Windows Server running in a cluster configuration. To enable SQL Cluster monitoring, you must perform the following configuration tasks:

1. Install the Operations Manager agent on every physical node in the cluster.
2. Enable Agent Proxy on all agent-managed computers in the cluster. Agent Proxy is enabled by clicking the **Allow this agent to act as a proxy and discover managed objects on other computers** option when editing the properties of an agent in the Agent Managed view in the Administration pane of the Operations console.
3. Configure the Windows Cluster Action Account Run As profile with an account that has administrative permissions for the cluster.

The Process of Configuring Monitoring for SQL Server

The System Center Management Pack for SQL Server provides support for versions of SQL Server listed in the following table.

The System Center Management Pack for SQL Server includes:

- Performance, health, and availability monitoring for all SQL Server components
- Performance views
- Database views
- Health state views
- SQL Server reports
- SQL Server tasks

Version	32-bit SQL Server on 32-bit OS	32-bit SQL Server on 64-bit OS	64-bit SQL Server on 64-bit OS
SQL Server 2005	√	√	√
SQL server 2008	√	√	√
SQL Server 2008 R2	√	√	√
SQL Server 2012	√	√	√

In addition, the following editions are supported:

- Datacenter
- Enterprise
- Developer
- Standard
- Express

Before Importing the System Center Management Pack for SQL Server

Before you import the System Center Management Pack for SQL Server, you must import the System Center Management Pack for Windows Server Operating System. This is because the System Center Management Pack for Windows Server Operating System monitors elements that SQL Server relies upon, such as memory, processor, and disk utilization.

Additionally, to use the SQL Server Management Studio task and SQL Server Profiler task that are both included with the System Center Management Pack for SQL Server, you must install SQL Server Management Studio and SQL Server Profiler on all computers running Operations Manager that will use the tasks.

Customizing the System Center Management Pack for SQL Server

As with all sealed Management Packs, it is recommended that you create a new Management Pack to store the customizations (overrides) required for the System Center Management Pack for SQL Server. A typical customization that is made after importing the System Center Management Pack for SQL Server is

to disable the SQL Server Full Text Search Service Monitor on all computers running SQL Server that do not have SQL Server Full Text Search installed.

Another typical customization that is performed when monitoring SQL Server on a cluster is to change the *Alert only if service startup is automatic* parameter from true to false. The reason for this is that by default, the System Center Management Pack for SQL Server monitors only services that are set to automatic. On cluster nodes, this would mean there would be no monitoring of critical SQL services, because the services' startup is set to manual. This customization should be performed on the following monitors:

- SQL Server Windows Service (for SQL DB Engine)
- SQL Server Reporting Services Windows Service
- SQL Server Analysis Services Windows Service
- SQL Server Integration Services Windows Service
- SQL Server Full Text Search Service Monitor
- SQL Server Agent Windows Service

Other common customizations include:

- **Enabling discovery of SQL Server Agent jobs.** Although long-running SQL Server Agent jobs are monitored by default in the System Center Management Pack for SQL Server, detailed monitoring can be provided only when SQL Server Agent jobs have been discovered. This option is disabled by default. To enable discovery of SQL Server Agent jobs, you must override the following monitors:
 - SQL Server 2012: Discover SQL Server 2012 Agent Jobs
 - SQL Server 2008: Discover SQL Server 2008 Agent Jobs
 - SQL Server 2005: Discover SQL Server 2005 Agent Jobs
- **Enabling job failure monitoring.** To enable alerts to be generated for failed jobs, you must enable the *A SQL job failed to complete successfully* monitor and select the "*Write to the Windows Application Event Log when the job fails*" option.
- **Modifying the discovery of SQL Server Database Engine instances.** By default, all SQL Server Database Engine roles are discovered and monitored by the System Center Management Pack for SQL Server. For security reasons, you might want to exclude specific SQL Server Database Engine roles from being discovered and monitored. In this scenario, you can specify an Exclusion List of SQL Server Database Engine instances that the discovery should ignore. To enable this, you override the following discoveries:
 - SQL Server 2012: Discover SQL Server 2012 Database Engines (Windows Server)
 - SQL Server 2008: Discover SQL Server 2008 Database Engines (Windows Server)
 - SQL Server 2005: Discover SQL Server 2005 Database Engines (Windows Server)
- **Modifying the discovery and monitoring of databases.** By default, all SQL Server databases are discovered and monitored by the System Center Management Pack for SQL. As with the Database Engine instance just described, you can also provide an Exclusion List for databases that you do not want discovered or monitored. To enable this, you override the following discoveries:
 - SQL Server 2012: Discover Databases for a Database Engine
 - SQL Server 2008: Discover Databases for a Database Engine
 - SQL Server 2005: Discover Databases for a Database Engine

Monitoring SQL Server in Secure Environments

In most organizations, the data that SQL Server stores is typically sensitive and is generally available only to the personnel or services that require access to it. Furthermore, the SQL Server that is hosting this data is locked down to ensure security. SQL Server has its own built-in security model, and SQL administrators use this to restrict access to databases and database instances. This can cause a problem with the System Center Management Pack for SQL Server. Consider the following scenario:

- You have installed System Center 2012 R2 Operations Manager and have configured Local System as the default action account.
- As a security measure, the SQL Server administrator has restricted the NT AUTHORITY\System account from the production SQL servers and has granted access only to specific accounts that require it. This is the default for all installations of SQL Server 2008.
- You deploy the System Center Management Pack for SQL Server but no SQL Server database engines or databases are discovered and monitored.

In this scenario, the default action account does not have access to the production SQL Server and so cannot discover and monitor SQL Server effectively. To resolve this issue, you must use the Run As accounts and Run As profiles in Operations Manager. Run As accounts and Run As profiles allow workflows in a Management Pack to run by using different credentials from those of the default action account. The System Center Management Pack for SQL Server provides three Run As profiles to assist with this:

- SQL Server Default Action Account
- SQL Server Discovery Account
- SQL Server Monitoring Account

To use these Run As profiles to distribute credentials to agent-managed computers hosting SQL Server, you must first create a Run As account that has the required permissions to discover SQL Server and a second, less-privileged Run As account to monitor SQL Server. You create Run As accounts from the Run As Configuration node in the Administration pane of the Operations console. When clicking the Accounts view under the Run As Configuration node, the Create Run As account task becomes available. This opens the Create Run As Account Wizard, which is used to create the Run As account. The following table describes the pages of the Create Run As Account Wizard, including the settings that should be configured to discover and monitor the computer hosting SQL Server in the preceding scenario.

Run As Account Wizard page	Description (based on the preceding example)
General Properties	On the General Properties page, you specify the Run As account type; in this case, Windows is selected. The display name for Production SQL Server Monitoring account is also provided.
Credentials	On the Credentials page, the user name, password, and domain for the account to be used are provided.
Distribution Security	On the Distribution Security page, the More secure option is selected. If the Less secure option is selected, the credentials will be distributed to all managed computers, which presents a security risk. By choosing the More secure option, you can control which agent-managed computers (computers hosting SQL Server) should receive the credentials.
Completion	After clicking Create, the Run As account is created, and the Run As Account Wizard completes.

After creating the Run As account, you must edit it from the Accounts view to specify the distribution settings. On the Distribution tab, you click Add to search for the computers that should receive the credentials, and then you add them to the Selected Objects window. After saving the changes, the credentials are distributed only to the computers added to the Distribution tab.

The Run As account can now be associated with the Run As profile. From the Profiles view in the Run As Configuration node, you can edit the SQL Server Default Action Account, SQL Server Discovery Account, and SQL Server Monitoring Account Run As profiles. When editing a Run As profile, you use the Run As Profile Wizard. Described in the following table are the pages of the Run As Profile Wizard and the settings that are configured for the scenario described earlier in this topic.

Run As Profile Wizard page	Description (based on the preceding example)
General Properties	On the General page, you specify a display name and optional description, and then select a Management Pack in which to store the configuration. In this case, where you are editing an existing Run As profile, this information has already been specified.
Run As Accounts	On the Run As Accounts page, you add the Run As account or accounts that will be associated with this Run As profile. It should be noted that if no Run As accounts are specified, the Default Action account is used. You must also select the objects that this Run As account will manage. In many cases, you can select the "All Targeted Objects" option so that wherever the Run As profile is associated with a workflow in the Management Pack, the Run As account will be used to run the workflow. In more complex scenarios, you can select the "A Selected Class, Group Or Object" option to select a specific class such as SQL Agent, a specific group such as SQL Server 2012 Computers, or a specific object such as MSSQLSERVER. In this scenario, where the workflows in the System Center Management Pack for SQL Server are associated with the relevant Run As profiles, the "All Targeted Objects" option is selected.
Completion	The changes to the Run As profile are saved by clicking the Save button.

In the simple scenario described earlier in this topic, the same Run As account was associated with all three Run As profiles. In more complex scenarios, where different credentials must be provided for different instances of SQL Server, the Run As profile can be configured with multiple Run As accounts, and the A Selected Class, Group Or Object option described earlier can be used to target those instances correctly. Similarly, the Run As account distribution settings would also be configured such that only the relevant computers running SQL Server received relevant credentials.

Monitoring SQL Server

After deploying the System Center Management Pack for SQL Server, a number of views are available in the Microsoft SQL Server folder in the Monitoring pane of the Operations console that are used to display the performance, health, and availability of all discovered instances of SQL Server, including any associated databases. Described in the following sections are some of the most commonly used views and reports.

Database Views

The following list describes Database views:

- **Database State.** The Database State view displays the health state of all discovered databases. This is useful because you can instantly determine whether any database is in an unhealthy state. When selecting a database, certain tasks become available, such as Check Database (DBCC) and Set

Database Offline. If installed, SQL Server Management Studio and SQL Profiler can also be opened from here.

- **Database Free Space.** The Database Free Space view is a performance view in which you can select either the Database DB Total Free Space (MB) or Database DB Total Free Space (%) counters to display a graph of the selected databases' free space. By right-clicking inside the graph area, you can use the Select Time Range feature to display free space for database over a given time period. Using this feature, you can become aware of trends in database sizes. The free space also takes into account whether the database is set to automatically grow and, if so, will include free space available on the disk when calculating total free space.
- **SQL Server 2012 Databases Summary Dashboard.** The SQL Server 2012 Databases Summary Dashboard displays the health state, database alerts, database details, database free space, and performance all within a single view. Selecting a database displays any warning or errors relating to the database. This is an ideal view to publish to a SharePoint, making it available to users who do not have access to the Operations console. Note that to use this dashboard, the SQL Server Management Pack must be downloaded from the Microsoft Download Center.

Health Monitoring Views

The following list describes health monitoring views:

- **Agent Health.** The SQL Agent Health view displays the health state for all SQL agents. If discovered, Agent Jobs are displayed in this view. Any related Agent Alerts are also displayed.
- **Database Engine Health.** The Database Engine Health view displays the health state and details for each discovered database engine. Also displayed are any Database Engine Alerts that have not been closed.

Performance Views

The following list describes performance views:

- **All Performance Data.** The All Performance Data view includes all performance counter data that has been collected from each computer running SQL Server. Counters include DB File Free Space (%) and Log Free Space (%). Use this view when you need to compare performance values across multiple instances of SQL Server, perhaps for capacity planning purposes.
- **Database Free Space.** The Database Free Space view provides the ability to create a graph of the free space in megabytes or as a percentage for each discovered SQL database. You can use this view to show how database size has changed over a given period of time. This will help with capacity planning, because you can predict (based on trend) when a database will run out of space.
- **Transaction Log Free Space.** The Transaction Log Free Space view displays the free space in both megabytes and as a percentage for each databases transaction logs.

Server Roles Views

The Server Roles Views include a health state view for each SQL Server role such as Analysis Services, Database Engine, Integration Services, and Reporting Services. When selecting a role instance in this view, tasks become available in the Tasks pane, including the Start and Stop task for the relevant role instance selected.

SQL Server Reports

Reports are included with the System Center Management Pack for SQL Server, including reports for SQL Database Space, SQL Server Lock Analysis, SQL Server Configuration, and SQL User Activity. Use these reports to obtain a historical view of how a computer running SQL Server has performed within a given time period. For example, you can use the SQL User Activity report to report on the number of logons per second over a given time period, such as during a particularly busy work period.

The Process of Configuring Monitoring for IIS Server

The System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8 provides monitoring for Internet Information Services (IIS) 8 running on Windows Server 2012, and Internet Information Services (IIS) 8.5 on Windows Server 2012 R2. The Management Pack supports monitoring in both a stand-alone or Network Load Balancing (NLB) environment.

The following Internet Information Services roles are monitored by this Management Pack:

- Web Sites
- Application Pools
- FTP Servers
- NNTP Servers
- SMTP Servers

Although no special configuration is typically required to use this Management Pack, the Management does require local administrative permissions on targeted computers so that it can discover and monitor IIS and run tasks against the computers. For this reason, many of the discoveries, monitors, and tasks are run under the context of the Privileged Monitoring Account Run As profile, which by default uses the Local System account.

Monitoring IIS Server

After installing the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8, a number of views become available within the Microsoft Windows Internet Information Services folder in the Monitoring pane of the Operations console. Described in the following list are some of the common views that are used to monitor the health performance and availability of IIS Server:

- **Web Site State.** The Web Site State view displays the health state of all discovered websites in IIS. You can use this view to instantly view any websites that are unhealthy. When selecting a website in this view, tasks become available in the Tasks pane, such Start Web Site, Stop Web Site, Enable Failed Request Tracing, and Disable Failed Request Tracing. You can use these tasks to troubleshoot issues with an IIS website without having to connect to the computer that is hosting the website.
- **Application Pool State, FTP Site State, IIS Computer State, and IIS Role State.** Similar to the Web Site State view, these views display the health state for all other IIS roles running on an IIS Server. Other tasks become available when selecting role instances in these views. For example, when you select an application pool in the Application Pool State view, you can use the Start Application Pool, Stop Application Pool, and Recycle Application Pool tasks.

Health Monitoring Views

Several health monitoring views, including FTP Server Health, FTP Site Health, Web Server Health, and Web Site Health, include both the health state and any relevant alerts for each IIS role. These views are useful when you need to correlate the health state of an IIS role with any alerts that have been generated for it. When you select a role instance, further information is included in the Detail view. For example, when you select a website in the Web Site Health view, the Details view displays information relating to

System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8 provides monitoring for:

- Website state
- Application pool state
- FTP site state
- IIS computer state
- IIS role state



the website, including useful troubleshooting data such as the Folder Path where the website is located, the Server Bindings, the Log File Pattern, and Anonymous Username, if applicable.

Performance Views

The Performance folder provides many performance views that you can use to determine the overall performance of web applications and each web server hosting them. For example, the Web Server Performance view displays a dashboard that displays the bytes sent, bytes received, and total bytes for the selected web server. When multiple web servers are selected, you can compare the values collected for each, which is useful when you need to determine how one web server is performing against another web server. Other performance views available include Web Site Performance, Processor Performance, SMTP Server Performance, and Memory Utilization (Physical).

The Process of Configuring Monitoring for SharePoint Server

The System Center Management Pack for SharePoint Server 2013 monitors the following SharePoint Server 2013 components:

- SharePoint Server
- Project Server
- Search Server

Before installing this Management Pack, you should ensure that the Operating System, SQL Server, and IIS Server Management Packs are already installed and that relevant components are discovered. The System Center Management Pack for SharePoint Server 2013 relies on these components to discover and monitor SharePoint Server 2013.

The System Center Management Pack for SharePoint Server 2013 provides:

- Performance, health, and availability monitoring for SharePoint Server, Project Server, and Search Server
- Performance views
- Health State views
- Alert views
- Unidentified Machine view



Unlike most Management Packs, the System Center Management Pack for SharePoint Server 2013 requires some initial configuration before SharePoint Server 2013 can be discovered and monitored. Configuration includes creating a Run As account, editing a configuration file, and running the Configure SharePoint Management Pack task that is included with the Management Pack. Described in the following table are the configuration steps that you must perform after installing the System Center Management Pack for SharePoint Server 2013.

Configuration steps for the System Center Management Pack for SharePoint Server 2013

Follow these steps to configure System Center Management Pack for SharePoint Server 2013:

1. **Create a Management Packs folder on the Management Server.** On the computer hosting the Operations Manager Management Server role, create a folder named **System Center Management Packs** in the C:\Program Files folder.
2. **Copy the configuration file.** From the location where the Management Pack was extracted (by default, this is C:\Program Files (x86)\System Center Management Packs), copy the Microsoft.SharePoint.foundation.library.mp.config file to the C:\Program Files\System Center Management Packs folder created in the previous step.
3. **Create a Run As account.** Create a Run As account named **SharePoint Discovery/Monitoring Account** by using the Windows Run As account type. It is important to use this name precisely for the Run As account, because it is referenced in the configuration file. If required, you can modify the configuration file to use a different Run As account name, but that name must match the one created in Operations Manager exactly. Ensure the account specified in the Run As account has SharePoint

Server 2013 Farm Admin rights and has full access to all SharePoint databases. Ensure the More Secure option is selected when creating the Run As account. After creating the Run As account, edit the Distribution tab, and add the relevant servers that form the SharePoint Farm and the computers hosting the SQL Server that include the SharePoint Farm databases.

4. **Edit the configuration file to include the SharePoint Servers.** Edit the Microsoft.SharePoint.foundation.library.mp.config file, and under the <Association Account="SharePoint Discovery/Monitoring Account" Type="Agent"> section, add the fully qualified domain name (FQDN) of each server in the SharePoint farm. For example, if one of the servers is named SharePoint1.contoso.com, add a line as follows:

```
<Machine Name="SharePoint1.contoso.com" />
```

Save the configuration file after including all servers in the SharePoint farm.

5. **Run the Configure SharePoint Management Pack task.** In the Monitoring pane, expand the Microsoft SharePoint folder, and then click Administration. In the details pane, click Microsoft SharePoint Farm Group, and then in the Tasks pane, click Configure SharePoint Management Pack. Click Run, and then monitor the Task Status window until a message appears in the Task Output box stating that the SharePoint Management Pack configuration completed successfully. Then, close the Task Status window.

After you complete the configuration, the relevant SharePoint components will be discovered. This can take up to 40 minutes to complete. After 40 minutes, check the Servers view in the Microsoft SharePoint folder to confirm the relevant SharePoint Servers have been discovered.

Monitoring SharePoint Server 2013

After you install and configure the System Center Management Pack for SharePoint Server 2013 and the various components have been discovered, views are available within the Microsoft SharePoint folder in the Monitoring pane of the Operations console. You use these views to monitor the health, performance, and availability of SharePoint Server 2013. Some of the most commonly used views are described in the following sections.

State View

State views display the current health state of all discovered SharePoint Server 2013 components. These views include the following:

- Configuration Databases
- Content Databases
- Farms
- Servers
- Service Front Ends
- Services
- Shared Services
- SPHA Rules
- Web Applications

Alert and Event View

The Active Alerts view displays alerts relating to all SharePoint Services. As with all alert views, you can view the alert properties to obtain detailed information relating to the alert, including symptoms and

possible resolutions. The Events view displays any events collected from all SharePoint Server 2013–monitored components.

Unidentified Machines View

The Unidentified Machines view is typically empty. However, if this view displays servers that have not been discovered in the SharePoint farm, Operations Manager likely does not have sufficient permissions on the SharePoint servers. You should check the Run As account as described earlier, and confirm that this account has the necessary permissions on the servers listed in this view.

Demonstration: Configuring Base Operating System Monitoring

In this demonstration, you will learn how to import the Base Operating System Management Pack and use several of the health monitoring views that are included with it.

Demonstration Steps

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Use the Import Management Packs wizard to install all the Management Packs in the following location:

\LON-DC1\Media\Additional Management Packs\Windows Server Operating System\Windows Server 2012 R2.

3. Use the following views to confirm the operating system on LON-DC1 has been discovered and is in a healthy state:
 - Windows Server State
 - Health Monitoring\Operating System Health
 - Health Monitoring\Disk Health

Question: You are planning to install the System Center Management Pack for SQL Server in your environment. You are aware that the SQL Server database administrators have locked down the SQL Server for security purposes and have removed the local system account from the SQL security settings. What should you do?

Lesson 3

Configuring Network Device Monitoring

Monitoring the network infrastructure is as important as monitoring the applications and components that it relies on. If you do not monitor the network infrastructure, it can be difficult to locate application issues in the environment. For example, consider a .NET web application that requires access to a SQL Server database that is hosted on a computer running Windows Server 2012.

End-users access the application and receive a “database not found” error message. You view the Operations console, and an alert is generated stating that the .NET web application has lost contact to the server running SQL Server. You check the health state of the server running SQL server and it shows that the server is healthy.

In this scenario, the port on the network device that connects the server running SQL server to the .NET application server is unavailable. However, if the device is not visible, detecting this as the cause of the issue would be challenging.

If the network device is monitored by Operations Manager, an additional alert is shown in the Operations console. The alert states that the port on the monitored network device is unavailable. By enabling network device monitoring in Operations Manager, you complete the end-to-end monitoring of applications and services that run in the datacenter or the private cloud.

You must understand how network monitoring is configured in Operations Manager, including how network devices are discovered.

Lesson Objectives

After completing this lesson, students will be able to:

- Configure network device discovery in Operations Manager.
- Monitor network devices.
- Use the network monitoring dashboards.
- Use the network monitoring reports.

How Operations Manager Discovers Network Devices

Network device monitoring is significantly improved in System Center 2012 R2 Operations Manager. Network device monitoring now includes several new reports and views, including dashboard views that are provided out of the box. Discovery, monitoring, and reporting of network devices for many vendors are provided, including the following vendors:

- Cisco
- F5
- Netscreen
- Juniper
- Nortel

Operations Manager provides support for multiple network devices by various vendors, including the following:

- Cisco
- F5
- Netscreen
- Juniper
- Nortel
- Nokia

Key components discovered are:

- Port/interface
- Processor
- Memory

- Nokia

Operations Manager can discover network devices by using SNMP 1, SNMP 2, and SNMP 3, and includes support for IPv4 and IPv6. For the devices that support it, extended monitoring of processor and memory monitoring is also provided.

More information about System Center Operations Manager 2012 and network devices with extended monitoring capability can be found at the following link:

 **System Center Operations Manager 2012: Network Devices with Extended Monitoring Capability**

<http://go.microsoft.com/fwlink/?LinkId=321893>

To discover network devices with Operations Manager, you can use the same Computer And Device Management Wizard that you use to deploy agents. You can also use the Discover Network Devices task that is available when you click Discovery Rules in Network Management of the Administration pane.

During the configuration of the discovery rule, follow these steps:

1. Select a Management Server that is dedicated to the discovery and a resource pool to use for monitoring the discovered devices.
2. Specify the discovery type (either Explicit or Recursive). When you use Explicit discovery, only the specified devices are discovered. However, when you use the Recursive option, the specified devices and the devices to which they are connected are discovered. This helps when the devices are combined with a scheduled discovery, because new devices are automatically discovered in the environment as they are added.
3. Select an existing, or configure a new, Run As account that is used to discover the network devices. This includes the SNMP community string that is used to communicate with the device.
4. Add the devices by using either the host name or the IP address. You can also import a list of devices from a text file. This helps when there are many devices to be discovered at the same time.
5. Use a schedule to discover the network devices, or run a discovery immediately. As soon as the configuration is complete, a discovery rule is created and can be viewed and edited in the Operations console, in the Network Management section of the Administration pane.

During discovery, Operations Manager discovers the components that are connected to the devices and their virtual local area network (VLAN) memberships and HSRP (Hot Standby Router Protocol) groups. It also discovers the association between IP ports and server network interface cards (NICs). This can help you troubleshoot network issues with an application server.

Important components of each network device that are discovered include the following:

- Port/interface
- Processor
- Memory

 **Note:** Only Management Servers or Gateway Servers can be used for discovery and monitoring of network devices. Additionally, each Management Server or Gateway Server can run only one discovery rule.

More information about how to discover network devices in Operations Manager, go to the following link:



How to Discover Network Devices in Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=321894>

Monitoring Network Devices

By default, after the network devices are discovered, the following components are monitored:

- Port/interface
- Processor
- Memory
- Connection Health
- VLAN Health
- HSRP Group

There are a number of views for network device monitoring, including the following:

- Active Alerts
- HSRP Groups
- Network Devices
- Routers
- Switches
- VLANs
- Health Explorer

Viewing Network Device Health

The Network Monitoring node in the Monitoring pane of the Operations console contains several views. These views can be used to determine the performance and availability of monitored network devices.

The Active Alerts view displays any related network device alerts, such as Interface Down or Network Device Is Not Responding. The Alert Description for the alert provides the device name or IP address that has caused the alert. Knowledge is also included in the Alert Details, which can help troubleshoot the issue.

There are several state views, including HSRP Groups, Network Devices, Routers, Switches, and VLANs, that can be used to view the health state of network devices. These views are used to obtain the quick overall health check of monitored devices.

The Health Explorer for the selected device can also be opened by right-click the device, clicking Open and then clicking Health Explorer. The Health Explorer contains detailed information about the monitors that are in a Warning or Critical health state, including summary information about what is being monitored, the configuration, and the causes of possible error states for the monitor. The Summary information also includes the Resolutions, which describe how to resolve a monitor that is in a critical or warning state. The State Change Events tab in the Health Explorer can be used to match network device issues to other issues that have occurred in the environment, for example, a date and time when the monitor's state changed from Healthy to Unhealthy.

Several Performance views exist. These views include Free Memory (Percent), ICMP Ping Response Time (Milliseconds), Interface Usage Statistics, Port Usage Statistics, and Processor Utilization (Percent). The performance views are helpful when you want to view performance data for a device in a specified time period. For example, network performance might be reduced during a specific time of day. You can use these performance views to display performance statistics during the same period to determine what is causing poor network performance.

Providing High Availability in Network Device Monitoring

Network Device monitoring supports resource pools. *Resource pools* use a pool of Management Servers to provide high availability for network device monitoring. If a Management Server in a resource pool stops responding, the network device monitoring it is providing will be automatically distributed to other management servers in the resource pool.



Note: By default, only ports that connect two monitored network devices together, and ports to which a managed server is connected, are monitored. This is by design so that monitoring is not enabled on ports that are not being used. You can change the monitoring to include additional ports.

Adding Network Device Monitors to a Distributed Application Diagram

To complete the end-to-end monitoring for a Distributed Application Diagram, you can add the related network devices that an application or service relies upon to the Distributed Application Diagram. In the Distributed Application Designer, you add a component group that is targeted at the Network Device class from the Device group of the Logical Entity group. Discovered network devices are then listed and then you can add the related devices to the component group. As with other component groups, the relationship and health rollup can also be configured. Therefore, when you use the Diagram view to monitor the health of an application, you can also view the health and availability of the network devices. This includes how the network devices are connected to one another and the application that is being monitored.

Network Monitoring Dashboards

Included with the Networking Monitoring Management Pack are several dashboards. The dashboards show you how the network is configured and monitored. Dashboards are described in the following sections.

Network Summary Dashboard

The Network Summary Dashboard view provides information that relates to the following:

- Nodes with slowest response (ICMP ping)
- Nodes with the highest CPU usage
- Interfaces with the highest utilization
- Interfaces with the most send errors
- Interfaces with the most receive errors
- Nodes with the most alerts
- Interfaces with the most alerts

Network monitoring dashboards include the following:

- Network Summary
- Network Node
- Network Interface
- Network Vicinity

The Network Summary dashboard can be opened from the Network Monitoring node in the Monitoring pane. You can use this dashboard to provide a summary of the network performance and availability in the past 24 hours.

Network Node Dashboard

The Network Node Dashboard view provides information about the following:

- Vicinity view of the node
- Availability statistics of the node in the past 24 hours, past 48 hours, past 7 days, or past 30 days
- Node properties
- Average response time of the node

- Processor usage of the node in the past 24 hours
- Current health of interfaces on the node
- Alerts generated by this node
- Alert details

You can open the Network Node Dashboard by clicking the Network Node Dashboard link in the Tasks pane. When you select a network device in the Monitoring pane, this link becomes available. You can use this dashboard to view the performance and availability of a single network device. The dashboard also displays the device details, such as the SNMP Agent Address, Model, and Location.

Network Interface Dashboard

The Network Interface Dashboard view provides information about the following:

- Bytes sent and received over the past 24 hours
- Packets sent and received over the past 24 hours
- Interface properties
- Send and receive errors and discards over the past 24 hours
- Network interface usage percentage
- Alerts generated by this interface
- Alert details

You can open the Network Interface Dashboard by selecting the Network Interface Dashboard task. However, an interface must be selected from the Health of interfaces list in the Node section in the Network Node Dashboard. You can use this dashboard to obtain interface utilization in the past 24 hours. This can help troubleshoot poor network performance that is caused by overused network interfaces.

Network Vicinity Dashboard

The Network Vicinity Dashboard view can be used to display monitored network devices and agent-managed computers. This includes how the devices and/or agent-managed computers are connected to one another. You can use this dashboard to view the network topology of monitored network devices. You can increase the hop count up to five hops and also include computers in the dashboard. The Network Vicinity Dashboard can be opened by selecting the Network Vicinity task when the Network Devices view is selected in the Monitoring pane.

More information about how to view network devices and data in Operations Manager can be found at the following link:

Viewing Network Devices and Data in Operations Manager

<http://go.microsoft.com/fwlink/?LinkID=321895>

Network Monitoring Reports

Reports available when monitoring network devices with System Center 2012 R2 Operations Manager include the following:

- **Memory Utilization.** The Memory Utilization report shows the percentage of free memory over time for a network device.
- **Processor Utilization.** The Processor Utilization report shows the processor utilization over time for a network device.
- **Interface Traffic Volume.** The Interface Traffic Volume report shows the rate of incoming and outgoing traffic over time for a selected port or interface.
- **Interface Error Packet Analysis.** The Interface Error Packet Analysis report shows the percentage of packets that are discarded or in error for both incoming and outgoing traffic for the adapter.
- **Interface Packet Analysis.** The Interface Packet Analysis report shows the kinds of unicast or nonunicast packets that cross the selected port or interface.

Network Monitoring reports include the following:

- Memory Utilization
- Processor Utilization
- Interface Traffic Volume
- Interface Error Packet Analysis
- Interface Packet Analysis

You can use these reports to view the overall usage, performance, and availability of selected network devices. You can schedule these reports just as you can as other reports, by making them available to users on a network share. You can find the can be found in the Reporting pane in the Network Management Reports folder.

More information about reports for network monitoring in Operations Manager can be found at the following link:



Reports for Network Monitoring in Operations Manager

<http://go.microsoft.com/fwlink/?LinkID=321896>

Question: You have to view NIC statistics for a network device in the past 24 hours. What would be the best view to open in the Operations console?

Lesson 4

Configuring Fabric Monitoring

With the release of System Center 2012 R2 Operations Manager, a new Management Pack has been made available named the Fabric Management Pack. The Fabric Management Pack provides extensive monitoring for the network, storage, and compute resources that are utilized within Virtual Machine Manager and Microsoft Azure. It is important that you understand how the Fabric Management Pack is configured to monitor your Virtual Machine Manager and Microsoft Azure resources to help ensure the network, storage, and compute resources are available and performing optimally.

To understand and configure the Management Pack, it is important that you have a basic understanding of Virtual Machine Manager.

In addition to the Fabric Management Pack, System Center Advisor provides ongoing configuration advice and tips for your core fabric components according to Microsoft best practices. This lesson explains how to configure fabric monitoring in Operations Manager.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe Virtual Machine Managers key features and functionality.
- Configure Operations Manager and Virtual Machine Manager Integration.
- Configure the Windows Azure Management Pack.
- Configure the System Center Management Pack for VMM Fabric Dashboard 2012 R2.
- Integrate Operations Manager with System Center Advisor.

Overview of System Center 2012 R2 Virtual Machine Manager

Virtual Machine Manager is Microsoft virtualization management solution. It provides support for the following virtualization technologies:

- Microsoft Hyper-V
- VMware ESX
- Citrix XenServer

Use virtual machine profiles in Virtual Machine Manager to quickly configure settings for virtual machines, such as the guest operating system, hardware, and applications. By using these profiles, you can create and deploy a virtual machine, or create a virtual machine template. You can also define virtual machine settings when you deploy services to private clouds. The following sections describe the provided Virtual Machine Manager profiles.

Guest Operating System Profile

Use the Guest Operating System profile to define the operating system, such as Windows Server 2008 R2 or Windows 8. If you configure the profile for Windows Server 2008 R2 or Windows Server 2012, you can configure the roles and features that should be made available, such as Active Directory Domain Services

Virtual Machine Manager provides management of the virtualized environment, including:

- Multiple virtualization host support Profiles
- Virtual machine templates
- Private clouds
- Service templates
- Live migration
- Power optimization



or SNMP Services. You can configure other settings, such as the computer name and domain to use when you deploy the virtual machine.

Hardware Profile

Use the Hardware profile to determine the virtual hardware that the virtual machine will use. This includes the processor, memory, disks, and network adapters. This includes the networks to which the network adapters connect. You also specify which virtualization hosts that the hardware profile will be compatible with, such as Hyper-V or ESX Server.

You can also configure CPU Priority and Memory Weight settings here. Virtual Machines with a higher priority are allocated resources before virtual machines with a lower priority.

You can also configure the hardware profile so that the virtual machines that use it are highly available. Then when VMM deploys the virtual machine, it will locate it on a virtualization server that is part of a cluster.

Application Profiles

Use Application profiles to determine the applications that will be deployed with the virtual machine. VMM can deploy virtualized applications that use packages that are created by Server App-V. Server App-V is a server application virtualization solution that is supplied as part of VMM. It resembles App-V, a desktop application virtualization solution. By making a server application virtual, VMM deploys it as a package when you deploy the virtual machine.

VMM can also deploy web applications that are packaged by using Microsoft Web Deploy. With Web Deploy you can export an IIS web application, and then use VMM to deploy it as part of the virtual machine. When you configure the package, you can also add parameters and normalize the application to make it generic. Then you can use the package in multiple environments, such as development and production, without creating a separate package for each environment.

VMM can also deploy SQL Server Data Tier Applications (DACs). A SQL DAC defines the database schema and objects that a database uses for an application. You can add multiple applications to an application profile and use scripts to control how they are deployed. For example, you can define a Post-Install script to run a script that updates antivirus product definitions after the application is deployed.

SQL Server Profile

Use the SQL Server profile to deploy SQL Server. By using Sysprep, you can create the operating system and SQL Server image that includes the required, relevant SQL features. When you deploy a virtual machine by using the SQL Server profile, VMM then configures SQL for the environment or service to which it is deployed.

Host Profile

The Host profile is used to deploy Windows Server to a computer and configure it with Hyper-V. The host is then automatically joined it to the domain so that VMM can use it as a virtualization host.

Private Clouds and Services

VMM lets you create private clouds, including the resources such as the virtualization hosts, logical networks, storage, CPU, and memory that the private clouds can consume. You then can deploy virtual machines and services to the private clouds using what is known as a Service Template, making applications and resources available to the cloud's users.

Think of a service in VMM as one or more virtual machine instances that include the hardware, software, and network configuration for the virtual machine. You can add multiple instances of virtual machines to a service, called a *multitier service*. Use virtual machine templates, which are created by using Virtual Machine profiles or by manual configuration, to quickly create a three-tier service, such as a database server, business application server, and web application server. You can then deploy the service to a

private cloud or virtualization host group. VMM uses placement rules to determine which virtualization hosts are best suited to host the virtual machines when you deploy the service.

When a service is deployed to a private cloud or host group, it can be scaled-out and scaled-in. Do this when you must increase the resources for a deployed service. For example, a marketing campaign might require the addition of two instances of the web application server. By using the scale-out feature, VMM can automatically deploy an additional two instances of the web application server tier.

VMM provides several other key features when you manage virtual machines, such as the ability to convert a physical computer into a virtual machine. It can also move virtual machines between virtualization hosts by using *live migration*. Live migration is also used in the VMM Power Optimization feature, where it can automatically move virtual machines and turn off underused virtualization hosts.

More information about System Center 2012 R2 Virtual Machine Manager can be found at the following website.



Virtual Machine Manager

<http://go.microsoft.com/fwlink/?LinkId=404085>

The Process of Configuring Integration Between Operations Manager and Virtual Machine Manager

By integrating Virtual Machine Manager with Operations Manager, you enable Operations Manager to monitor the virtual environment, which includes all components of Virtual Machine Manager, such as the VMM Server, the SQL database that it uses, and any virtual machines, services, and clouds that it manages.

In addition, by integrating VMM and Operations Manager, you can take advantage of the Performance and Resource Optimization (PRO) feature. With PRO-enabled Management Packs, Operations Manager can detect resource issues or hardware failures in the VMM environment, such as a virtualization host that is overused and results in poor performance. Through a PRO-tip, Operations Manager notifies the operator and recommends a strategy, such as migrating virtual machines to a different virtualization host. If it is configured to do so, this remediation can also be performed automatically without user intervention.

When VMM and Operations Manager are integrated, several additional views and tasks become available in the Operations console. These views and tasks let you view the health, performance, and availability of the VMM environment.

Virtual Machine Manager Views

In the Monitoring pane of the Operations console, you can use a number of views in the Virtual Machine Manager folder to determine the health and availability of VMM, including a view for Active Alerts and Health State. Use these views to gain a quick view of the health and availability of the VMM environment.

The Managed Resources folder contains several health state views that you can use to view the health of individual VMM components, such as the Cloud Health and Host Health views. Use these views to display the configuration of VMM components. For example, when you select a cloud in the Cloud health view, the cloud capability details are displayed in the Detail view. This view includes the Maximum VM Count, Maximum Storage, and Maximum Memory settings for the cloud.

Integrating Virtual Machine Manager with Operations Manager provides:

- Monitoring of the VMM environment
- Performance of VMM tasks from within the Operations console
- Performance and Resource Optimization (PRO)

The Performance folder contains performance views to monitor a component's current performance and performance over a selected period. For example, the Host Performance view displays performance counters that relate to bytes that are sent and received for the virtual network adapter. You can select these counters to display a graph that represents the bytes sent and received over the virtual network adapter. By using the Select Time Range option, you can set the time range of displayed data. This lets you see over time how much data was sent and received. This can also be useful in capacity planning. Other performance views include the following:

- Cloud Performance
- Service Performance
- Host Cluster Performance

Use the Diagram view in the Virtual Machine Manager Views folder to view the overall health of the VMM environment. By using a distributed application diagram, you can expand the components of VMM and instantly view the health of each. For example, by expanding the VMM Infrastructure component group, you can view the health of the VMM Server. By expanding the VMM Server component group, you can then view the health of the virtual machine guests, the VMM database, and any clouds that VMM manages.

You can also open the Health Explorer from any selected component in this view. Use this to troubleshoot failed monitors. A Summary, Causes, and Resolution section is displayed in the Health Explorer. This section displays State Change Events that you can use to match problems with other activities that have occurred in the VMM environment.

When you select a Virtual Machine in this view, several Virtual Machine tasks become available in the Tasks pane. Use these tasks to perform tasks against the selected virtual machine. For example, the Create Checkpoint task creates a checkpoint on the selected virtual machine. You can also perform other tasks such as Start, Stop, and Pause.

Configuring Integration

Before you integrate VMM and Operations Manager, you must install the following Management Packs in Operations Manager. The minimum version supported is also noted:

- SQL Server Core Library version 6.0.5000.0.
- Windows Server 2008 Operating System (Discovery) version 6.0.5000.0.
- Windows Server Operating System Library version 6.0.5000.0.
- Windows Server Internet Information Services Library version 6.0.5000.0.
- Windows Server Internet Information Services 2003 6.0.5000.0.
- Windows Server 2008 Internet Information Services 7 version 6.0.6539.0.

In addition, you must install the Operations Manager Operations console on the VMM Server before you configure the integration. It is also recommended that you deploy an Operations Manager agent to the VMM Server and on all virtual machine hosts before you configure integration.

To integrate VMM with Operations Manager, use the Add Operations Manager wizard that you open by double-clicking the Operations Manager Server setting in the System Center Settings node of the Settings pane in the VMM Administrator Console.

Listed in the following table are the pages and settings of the Add Operations Manager wizard.

Add Operations Manager wizard page	Description
Connection to Operations Manager	<p>On this page, you specify the server name of the Operations Manager Management Server that is used to connect to Operations Manager. You also specify the credentials to use to connect. By default, the VMM server service account is selected, but you can choose to use an existing Run As account or create a new Run As account. The account that is used here must be a member of the Operations Manager Administrators user role.</p> <p>You can also enable or disable PRO and maintenance mode. When hosts in VMM are put in maintenance mode, the hosts in Operations Manager are also put in maintenance mode. This stops the generation of any alerts while the hosts are being maintained.</p>
Connection to VMM	<p>On this page, you specify the credentials that Operations Manager should use when you connect to the VMM environment. The credentials that you use must be a member of the VMM Administrators user role.</p>

After completing the Add Operations Manager wizard, a VMM Jobs window opens in which you can view the status of the New Operations Manager connection job. When the job has completed, the relevant VMM Management Packs and associated views and tasks become available in the Operations console.

After the integration is configured, you can double-click the Operations Manager Server setting in the VMM Administrator console to view the status of the connection and update the connection. Use this setting when the Management Server in Operations Manager has been restarted. For example, for maintenance purposes.

The Process of Installing and Using the System Center Management Pack for VMM Fabric Dashboard 2012 R2

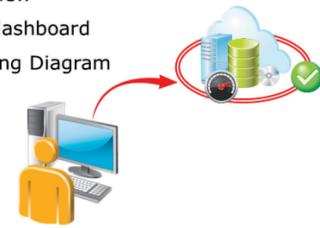
Before you can install the System Center Management Pack for VMM Fabric Dashboard 2012 R2, you must configure integration between Operations Manager and Virtual Machine Manager as described in the previous topic. This is because folders that are created during integration are reused by the System Center Management Pack for VMM Fabric Dashboard 2012 R2.

After configuring integration between Operations Manager and Virtual Machine Manager, you use the Import Management Packs wizard to import the System Center Management Pack for VMM Fabric Dashboard 2012 R2 into Operations Manager, just as you would any other Management Pack.

After importing the Management Pack there are a number of additional views and dashboards that become available in the Operations console to display the health, performance, and availability of the private clouds and fabric used to host them in Virtual Machine Manager. A description of each view and dashboard provided by the System Center Management Pack for VMM Fabric Dashboard 2012 R2 is included in the following sections.

The System Center Management Pack for VMM Fabric Dashboard 2012 R2 provides monitoring of private clouds and fabric in VMM and includes:

- Cloud Health view
- Fabric Health dashboard
- Fabric Monitoring Diagram



Cloud Health

The Cloud Health view displays the health state of all private clouds managed in VMM. For each private cloud, details such as the Health State, Name, Storage Classifications, Maximum VM Count, Maximum vCPU Count, Custom Quota, Maximum Storage, Maximum Memory, and the VMM Server managing the cloud are displayed. When you select a private cloud in this view, the details pane also displays information relating to the path in VMM where the cloud is stored, the Display Name, Description and, if relevant, the Cluster Name List.

The Cloud Health view is useful when you need to quickly determine the health state of any private cloud in VMM, because any private cloud in an unhealthy state is instantly displayed. Additionally, you can open other context-sensitive views by right-clicking a private cloud. For example, you can right-click a private cloud and then click Health Explorer to open the health explorer for that cloud. This is useful when troubleshooting an unhealthy private cloud, as you can instantly view the monitors that are in an unhealthy state and troubleshooting information relating to them. Other context-sensitive views that can be opened from here include the Alert View, Event View, and Performance View.

You can also open an Availability report for the selected cloud from here by right-clicking a cloud, clicking Report Tasks, and then clicking the Health report. The report opens, and the selected cloud is added to the report. You can then modify the report parameters, such as the From and To fields. When the report is run, it displays the availability of the cloud over the specified time period. This is useful when you need to know the availability of a private cloud between a start and end date. This can also be useful in obtaining service level agreement (SLA) information for the selected cloud.

Fabric Health Dashboard

When you select a private cloud in the Cloud Health view, the Fabric Heath Dashboard task becomes available in the Tasks pane. This task opens the Fabric Health Dashboard for the selected cloud. This is a very useful dashboard because it displays the health, availability, and alerts relating to the fabric used by the selected cloud, all within a single view. The following information relating the fabric used by the selected cloud is displayed:

- **Host State.** Provides the health state of the computing resources used by the cloud, such as Host Group, CPU, Memory, Disk, Network Adapters, and Number of VMs.
- **Storage Pool State and File Share and LUN State.** Provides the health state of the storage used by the cloud, including the disk space Capacity and % Allocated values.
- **Network Node State.** If Network Monitoring has been enabled, and monitoring for any physical network adapters that the cloud relies on has been configured, the health state of each network device is provided here. Virtual network devices are not included, however.
- **Active Alerts.** Any active alerts relating to the selected cloud or its underlying fabric are displayed here. Selecting an alert displays the alert details, including the Description, Source, and Path. Several Virtual Machine tasks also available when you select an alert, which can be useful when troubleshooting. Tasks include Create Checkpoint, Pause, Save State, Start, Stop, and Shutdown.

Fabric Monitoring Diagram

In the Microsoft System Center Virtual Machine Manager Views folder, in the Monitoring pane of the Operations console, you can open the Fabric Monitoring Diagram view. This view has been updated to include all relevant fabric resources in VMM. This view can be used to determine the health and availability for fabric resources such as the networking and storage components managed in VMM. As with other diagram views, various component groups can be expanded to display the health of subcomponents contained within the group. The health of each component is also updated, and because you can instantly determine the source of the problem, this feature helps you troubleshoot an issue with a specific fabric component. As described in the "Cloud Health" section earlier in this topic, you can also open other context-sensitive views from here, such as the Health Explorer view and Performance views.

Using a combination of the Virtual Machine Manager views, as described in the “The Process of Configuring Integration Between Operations Manager and Virtual Machine Manager” topic earlier in this module, and the dashboards and views just described, you can obtain detailed analysis of the health, performance, and availability of private clouds, including their underlying fabric resources.

The Process of Configuring the System Center Management Pack for Windows Azure

The System Center Management Pack for Windows Azure extends Operations Manager monitoring capabilities to include monitoring of fabric resources running in Microsoft Azure. When Operations Manager is integrated with Virtual Machine Manager and Microsoft Azure, you can use Operations Manager to monitor public and private cloud resources from within a single console.

The System Center Management Pack for Windows Azure provides the following functionality:

- Discovers cloud services running in Microsoft Azure
- Provides role instance health state
- Monitors and collects role instance performance information
- Monitors and collects role instance events
- Monitors and collects role instance Microsoft .NET Framework trace messages
- Grooms event, performance, and .NET Framework trace data from storage in Microsoft Azure
- Discovers storage in Microsoft Azure
- Discovers virtual machines in Microsoft Azure
- Monitors the size and availability of storage in Microsoft Azure
- Provides the health status of each role instance of virtual machines in Microsoft Azure
- Monitors certificates for the management and cloud service
- Includes dashboards for monitoring hybrid scenarios
- Includes a distributed application template for monitoring hybrid scenarios

The System Center Management Pack for Windows Azure provides:

- Monitoring for fabric resources hosted in Windows Azure
- Hybrid monitoring for both cloud and on-premise resources

Prerequisites for the System Center Management Pack for Windows Azure

Before you can install the System Center Management Pack for Windows Azure, the following perquisites must be in place:

- **Operations Manager.** You must be running System Center 2012 Service Pack 1 (SP1) Operations Manager or System Center 2012 R2 Operations Manager. Earlier versions are not supported.
- **Internet Connectivity.** To connect to the Microsoft Azure subscription, at least one Management Server in the Management Server resource pool must have access to the Internet.
- **Windows Azure Diagnostics.** Windows Azure Diagnostics must be enabled in Microsoft Azure and must be configured to forward data to Microsoft Azure storage.

Configuring the System Center Management Pack for Windows Azure

After importing the System Center Management Pack for Windows Azure, you must configure the Management Pack to first discover the Microsoft Azure resources that you want to monitor, and then use the Windows Azure Monitoring Management Pack template to configure monitoring of the discovered resources. This is required because, unlike most Management Packs, monitoring does not start automatically with the System Center Management Pack for Windows Azure.

Before you can connect and discover Microsoft Azure resources from Operations Manager, you must upload a valid x509 certificate to the Microsoft Azure development portal. This enables the use of the Microsoft Azure Management application programming interface (API).

To discover Microsoft Azure resources in Operations Manager, you use the Add Windows Azure Subscription wizard. After you import the System Center Management Pack for Azure, this wizard becomes available in the Windows Azure node in the Administration pane in the Operations console. When working through the Add Windows Azure Subscription wizard, you must supply the Microsoft Azure information described in the following table.

Add Windows Azure Subscription wizard page	Description
Subscription Configuration	On the Subscription Configuration page, you supply the subscription ID, the certificate file, and the password for the certificate specified. At this stage, the wizard attempts to connect to the specified Microsoft Azure subscription to confirm the details you entered were correct.
Server Pool	On the Server Pool page, you select a valid Management Server resource pool that has Internet access. You can optionally include the address of a proxy server if one is required for Internet access. After completing this page, you click Add Subscription.
Summary	On the Summary page, you are shown the various settings that have been configured. If necessary, you can go back through the wizard and make changes. After confirming all settings, you click Add Subscription to connect Operations Manager to the Microsoft Azure subsection.

After configuring the subscription information, Operations Manager will start discovering the Microsoft Azure resources. To confirm resources have been discovered correctly, you can use the various views provided in the Azure Resource Inventory folder, which is available in the Windows Azure folder in the Monitoring pane in the Operations console. Views include Discovered Cloud Services, Discovered Storage, and Discovered Virtual Machines. Additionally, from within the Other Azure Inventory subfolder, you can access the Discovered Deployments, Discovered Role Instances, Discovered Roles, Discovered Sql Azure Instances, and Discovered Subscriptions views, which show other discovered Microsoft Azure resources.

Configuring Monitoring of Microsoft Azure Resources

After Operations Manager has discovered the Microsoft Azure resources, you can use the Windows Azure Monitoring Management Pack template to configure the monitoring of them. The template is available from within the Management Pack Templates node in the Authoring pane of the Operations console. To configure the Windows Azure Monitoring Management Pack template, you use the Add Monitoring Wizard, which is available in the Authoring pane, and then select the Windows Azure Monitoring template. In the following table, a description of each page of the Add Monitoring Wizard is provided, including the settings configured for the Windows Azure Monitoring Management Pack template.

Add Monitoring Wizard page when configuring the Windows Azure Monitoring Management Pack template	Description
General Properties	On the General Properties page, you supply a name for the monitor that is being created and an optional description. You must also select an unsealed Management Pack in which the configuration will be saved. Creating a new Management Pack to store this configuration in is recommended.
Subscription	On the Subscription page, you select the subscription for which you will include monitoring. Note that only subscriptions successfully configured by using the Add Windows Azure Subscription wizard are displayed here.
Cloud Services	On the Cloud Service page, you add and search for cloud services and deployments that you wish to provide monitoring for.
Virtual Machines	On the Virtual Machines page, you add and search for virtual machines that you want to provide monitoring for.
Storage	On the Storage page, you add and search for storage that you want to provide monitoring for.
Summary	On the Summary page, you can review your selections and then amend them as necessary. You then click Create to create the monitor.

Monitoring Microsoft Azure Resources

The Windows Azure folder and Monitored Azure Resources folder in the Monitoring pane of the Operations console provide a number of views that can be used to display the health, performance, and availability of monitored Windows Azure resources. For example, in the Windows Azure folder, the Active Alerts and All Alerts Last 24 Hours views can be used to view any alerts relating to monitored Microsoft Azure resources. There is also a Service State view, which displays the health state of all monitored Microsoft Azure services.

A Topology Dashboard is provided, which shows the relationship between Microsoft Azure objects in the monitored subscription. The Topology Dashboard is particularly useful because it displays all cloud services and allows you to filter the dashboard based on subscription or deployment slot, such as production or staging. Other views available in the Monitored Azure Resources folder include Cloud Service State, Storage State, Virtual Machine State, Deployment Slot State, Role Instance State, Role State, and Subscription State.

A number of performance views are also included in the Performance folder, including ASP.NET Performance, Disk Capacity, Memory Utilization (Physical), Network Adapter Utilization, Processor Performance, Role Instance Performance (All Counters,) and Storage Account Size.

To assist with monitoring hybrid scenarios in which you have resources both in the cloud and on the premises, a new Distributed Application Diagram template named Windows Azure Distributed Application is also provided. Using this template, you can quickly add discovered resources from both cloud and on-premise applications to provide hybrid monitoring within a single view. Distributed applications and distributed application diagrams are covered in detail later in this course.

The Process of Configuring Integration Between Operations Manager and System Center Advisor

System Center Advisor is an online service hosted in Microsoft Azure that analyzes Microsoft server software for potential issues such as missing security patches. It also compares the configuration of these servers against best practice guidelines created by Microsoft support engineers and the Microsoft System Center Advisor product group.

If an issue is detected by System Center Advisor, an alert is generated to identify the problem. Similarly, if a configuration drift from best practice is detected, remediation advice can also be viewed.

The System Center Advisor environment is not dissimilar to an Operations Manager environment and consists of the components described in the following table.

System Center Advisor component	Description
Agents	A System Center Advisor agent is installed on the on-premise Windows-based servers that you want to use for collecting data for analysis. Data is collected and analyzed by the agent by using rules similar to those found in an Operations Manager Management Pack. In System Center Advisor, these rules are known as <i>Advisor knowledge</i> .
Gateways	A gateway is installed on an on-premise server to collect data from agents and then upload that data to the System Center Advisor web service running in Microsoft Azure.
Advisor Console	The data is analyzed and aggregated in Microsoft Azure, and then made available through a Web console known as the <i>Advisor console</i> .

Alerts and any remediation advice can then be viewed in the Advisor console.

Configuring Integration Between Operations Manager and System Center Advisor

In System Center 2012 SP1 Operations Manager, you needed to download the System Center Advisor Connector and import Management Packs before integration could be configured. Additionally, your Operations Manager environment had to be running at least Update Rollup 2 for Operations Manager 2012 SP1. In System Center 2012 R2 Operations Manager, System Center Advisor support is built in, making configuring integration much quicker and easier.

To configure integration, in the Administration pane, expand the System Center Advisor node, and then select Advisor Connection. This makes the Register To Advisor Service link available in the details pane. Click the link to open the Register To Advisor Service wizard, in which you supply the Microsoft account details that were used when you registered the System Center Advisor subscription.

After you register with the System Center Advisor service, you must add into Operations Manager the computers that System Center Advisor is managing. You do this by using the Advisor Managed view in the System Center Advisor node in the Administration pane of the Operations console.

Integrating Operations Manager with System Center Advisor involves:

- Registering with the System Center Advisor service
- Adding computers managed by System Center Advisor into Operations Manager

When integration is configured, you can:

- View System Center Advisor alerts in Operations Manager
- View configuration of managed servers
- View remediation advice for alerts generated by System Center Advisor

After clicking the Advisor Managed view, an Add a Computer Group task becomes available in the Tasks pane. This task opens a Computer Search window where you can add computers and groups that Operations Manager will collect System Center Advisor alerts from.

Viewing System Center Advisor Alerts in Operations Manager

After you register with the System Center Advisor service and add the computers and group you want to collect System Center Advisor alerts from, you can view alerts collected from the Active Alerts view in the System Center Advisor folder in the Monitoring pane of the Operations console. When you select an alert, you can view related information, such as the computer or instance that generated the alert, and any recommended remediation for addressing the issue that caused the alert to be generated. There are also four tasks made available in the Tasks pane:

- **Ignore Alert.** This task can be used to ignore the alert from the server that generated it, or ignore the alert from all servers managed by System Center Advisor.
- **Manage Alert Rules.** This task can be used to view all rules used by System Center Advisor. You can clear the selection of any rules from here if you do not want System Center Advisor to generate an alert for them.
- **View Configuration.** This task can be used to view the configuration information collected for the server that generated the alert. This can be a useful troubleshooting tool, because you can correlate configuration information with alerts generated by System Center Advisor to help determine the cause of the alert.
- **View Solution/KB Article.** This task can be used to display remediation information relating to the selected alert. A Knowledge Base article is displayed that provides more information about the alert, including the symptoms and relevant resolution steps you can take to resolve the issue.

More information about System Center Advisor can be found at the following website.



System Center Advisor

<http://go.microsoft.com/fwlink/?LinkID=507760>

Question: You are configuring integration between Operations Manager and Virtual Machine Manager. What should you install on the Virtual Machine Manager Server to integrate VMM with Operations Manager?

Lab: Configuring Application and Fabric Monitoring

Scenario

After installing Operations Manager and deploying agents to the application servers for Contoso, Ltd., you must now configure monitoring for them. You must install a number of base Management Packs, including Windows Operating System, IIS Server, SQL Server, and SharePoint Server. Access to many of the databases running SQL Server is secured with separate security credentials. For this reason, you must also configure the SQL Run As account and Run As profile so that the Operations Manager agent can monitor the databases effectively. In addition, because Contoso manages their virtualization environment by using Virtual Machine Manager and has virtual machines running in Microsoft Azure, you must also configure integration between Operations Manager and Virtual Machine Manager, and between Operations Manager and Microsoft Azure, so that you can monitor the network, storage, and compute resources in both your private and public cloud environments. This process includes configuring the VMM Fabric Dashboard for visibility of your public and private cloud resources.

Objectives

After completing this lab, you will be able to:

- Install the System Center Management Pack for Windows Server Operating System.
- Install and configure the System Center Management Pack for SQL Server.
- Install the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8.
- Install and configure the System Center Management Pack for SharePoint Server 2013
- Configure network monitoring.
- Configure integration between Operations Manager and Virtual Machine Manager.

Use the System Center Management Pack for VMM Fabric Dashboard 2012 R2.Lab Setup

Estimated Time: 60 minutes

Virtual Machines: 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-MS2, 10964C-LON-AP2, 10964C-LON-AP1, 10964C-LON-SC1

User Name: Contoso\Administrator

Password: Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, In Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Domain: **Contoso**
5. Repeat steps 2–4 for the following virtual machines:

- 10964C-LON-SQ1 (On LON-HOST1)
- 10964C-LON-MS1 (On LON-HOST2)
- 10964C-LON-MS2 (On LON-HOST1)
- 10964C-LON-AP1 (On LON-HOST1)
- 10964C-LON-AP2 (On LON-HOST2)
- 10964C-LON-SC1 (On LON-HOST2)

 **Note:** Before starting this lab, make sure that all Windows Services that are set to start automatically are running, except for the Microsoft .NET Framework NGEN v4.0.30319_X86 and.NET Framework NGEN v4.0.30319_X64 services, because these services stop automatically when they are not in use.

Exercise 1: Installing the System Center Management Pack for Windows Server Operating System

Scenario

To monitor the Windows Server-based operating systems in the Contoso IT environment, you must install the System Center Management Pack for Windows Server Operating System. After installing the Management Pack, you must confirm that the operating systems have been discovered by Operations Manager and confirm that they are in a healthy state.

The main tasks for this exercise are as follows:

1. Install the System Center Management Pack for Windows Server Operating System
2. Confirm the operating systems have been discovered and monitored

► Task 1: Install the System Center Management Pack for Windows Server Operating System

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Use the Import Management Packs wizard to install all the Management Packs in the following location:

\LON-DC1\Media\Additional Management Packs\Windows Server Operating System\Windows Server 2012 R2.

► **Task 2: Confirm the operating systems have been discovered and monitored**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Microsoft Windows Server

2. Use the following views to confirm the Operating System on LON-SQ1 has been discovered and is in a healthy state:
 - o Windows Server State
 - o Health Monitoring\Operating System Health
 - o Health Monitoring\Disk Health



Note: It may take up to 10 minutes for the Operating System to be discovered.

Results: After this exercise, you should have installed the System Center Management Pack for Windows Server Operating System and confirmed that the operating systems have been discovered and are in a healthy state.

Exercise 2: Installing and Configuring the System Center Management Pack for SQL Server

Scenario

To monitor the servers running SQL Server at Contoso, you must install and configure the System Center Management Pack for SQL Server. These servers have been locked down, so you will also need to configure a Run As account to discover and monitor them effectively.

The main tasks for this exercise are as follows:

1. Create a SQL Server monitoring account
2. Create a Run As account
3. Create a group
4. Install the System Center Management Pack for SQL Server
5. Configure the Run As profiles
6. Configure permissions on the computer running SQL Server
7. Confirm SQL monitoring

► Task 1: Create a SQL Server monitoring account

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-DC1
Tool	Active Directory Users and Computers
OU	SCOM2012
User	SQLMonitoring

2. Create a new user in the SCOM2012 container with the following properties:

- User name: **SQLMonitoring**
- Password: **Pa\$\$w0rd**
- Password Never Expires: **True**
- User must change password at next logon: **False**

► Task 2: Create a Run As account

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration

Location	Value
View	Run As Configuration\Accounts

2. Create a new Run As account with the following properties:
 - Name: **SQL Monitoring Account**
 - Account Type: **Windows**
 - User name: **SQLMonitoring**
 - Password: **Pa\$\$w0rd**
 - Distribution Security: **More secure**
3. Edit the **SQL Monitoring Account** Run As account, and on the **Distribution** tab, add the **LON-SQ1.CONTOSO.COM** computer.

► **Task 3: Create a group**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Authoring
View	Groups

2. Create a new group with the following settings. All other settings should remain the default settings.
 - Name: **Contoso SQL Servers**
 - Management Pack: Create a new Management Pack named **Contoso SQL Servers**
 - Explicit Members: Search for **Windows Computers**, and then add **LON-SQ1.CONTOSO.COM**

► **Task 4: Install the System Center Management Pack for SQL Server**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Use the Import Management Packs wizard to install all the Management Packs in the following location:
 \\LON-DC1\Media\Additional Management Packs\SQL Server.

► **Task 5: Configure the Run As profiles**

- To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Run As Configuration\Profiles

- Edit the following profiles, and add the **SQL Monitoring Account** Run As account. When adding the account, use the **Select A selected class, group or object** and **Group** options, and then select the **Contoso SQL Servers** group.

- SQL Server Default Action Account**
- SQL Server Discovery Account**
- SQL Server Monitoring Account**

► **Task 6: Configure permissions on the computer running SQL Server**

- To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-SQ1
Tool	Computer Management
View	Local Users and Groups
Group	Administrators

- Add the **SQLMonitoring** account to the local Administrators group on LON-SQ1.

► **Task 7: Confirm SQL monitoring**

- To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Microsoft SQL Server

- Review the information in the following views to confirm SQL Server has been discovered and is being monitored:

- Databases\Database State

- SQL Agent\SQL Agent State
- Server Roles\ Database Engines
- Server Roles\ Reporting Services

 **Note:** It may take up to 15 minutes for the SQL Server components to be discovered. You can continue with the next task before the components are discovered.

Results: After this exercise, you should have installed the System Center Management Pack for SQL Server. You will have created a Run As account for discovering SQL Server and associated it with the relevant SQL Server Run As profiles.

Exercise 3: Installing the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8

Scenario

Contoso has a number of business-critical web applications that staff members use to perform their jobs. It is important for these web applications to be available at all times and to perform at optimum levels. To facilitate effective monitoring for these applications, you must install the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8.

The main tasks for this exercise are as follows:

1. Install the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8
2. Confirm IIS monitoring

► Task 1: Install the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8

1. To perform this task, use the computer and tool information in the following table

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Use the **Import Management Packs** wizard to install all the Management Packs from the following location:
 - \\LON-DC1\Media\Additional Management Packs\Internet Information Services 8
3. Use the **Import Management Packs** wizard to install all the Management Packs except the **Microsoft.Windows.InternetInformationServices.CommonLibrary.mp** from the following location:
 - \\LON-DC1\Media\Additional Management Packs\Internet Information Services 7

► **Task 2: Confirm IIS monitoring**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Microsoft Windows Internet Information Services

2. Use the following views to confirm IIS has been discovered and is being monitored:

1. IIS Role State
2. Web Site State
3. Application Pool State



Note: It may take up to 15 minutes for the IIS components to be discovered.

Results: After this exercise, you should have installed the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8 and confirmed that the web applications were discovered and monitored.

Exercise 4: Installing and Configuring the System Center Management Pack for SharePoint Server 2013

Scenario

Contoso uses SharePoint Server 2013 to share business-critical information with personnel in the organization. To ensure the SharePoint environment is always available and performing at optimum levels, you must install and configure the Center Management Pack for SharePoint Server 2013.

The main tasks for this exercise are as follows:

1. Install the System Center Management Pack for SharePoint Server 2013
2. Configure the System Center Management Pack for SharePoint Server 2013
3. Confirm SharePoint monitoring

► Task 1: Install the System Center Management Pack for SharePoint Server 2013

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Use the Import Management Packs wizard to install all the Management Packs in the following location:

\\LON-DC1\Media\Additional Management Packs\ SharePoint Server

► Task 2: Configure the System Center Management Pack for SharePoint Server 2013

1. To perform this task, use the computer and tool information in the following table

Location	Value
Computer	LON-MS1
Tool	Windows Explorer
Folder	C:\Program Files
Folder to create	System Center Management Packs

2. Create the **System Center Management Packs** folder in the **C:\Program Files** folder, and then copy the **Microsoft.SharePoint.foundation.library.mp.config** file from the **LON-DC1\Media\Additional Management Packs\SharePoint Server** folder to the **C:\Program Files\System Center Management Packs** folder.
3. In the Operations console, create a new Run As account named **SharePoint Discovery/Monitoring Account**, and then associate the **Contoso\Administrator** account with it.
4. Edit the **Distribution** of the Run As account so that the account is distributed only to LON-AP1.CONTOSO.COM.

- From the **Monitoring** pane, open the **Microsoft SharePoint\Administration** view, and then run the **Configure SharePoint Management Pack** task.

 **Note:** If the task fails, wait for 5 minutes and then run the task again. This is due to SharePoint objects being discovered.

 **Note:** The Microsoft SharePoint Farm Group may be displayed in a **Not monitored** state. This is normal as discovery of all SharePoint resources has not completed yet.

► Task 3: Confirm SharePoint monitoring

- To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Microsoft SharePoint

- From the **Microsoft SharePoint** folder, open the following views to confirm SharePoint Server 2013 has been discovered and is being monitored:

- Servers
- Service Front Ends
- Shared Services
- Diagram View
- Web Applications

 **Note:** Some components may be in a warning or critical state. This is expected and confirms that the SharePoint Management Pack is monitoring SharePoint.

 **Note:** It can take up to 30 minutes for all SharePoint components to be discovered.

 **Note:** Some websites may be in a warning or critical state. This is expected and confirms that the SharePoint Management Pack is monitoring SharePoint.

Results: After this exercise, you should have installed and configured the System Center Management Pack for SharePoint Server 2013. You should also have confirmed that Operations Manager discovered the SharePoint environment and monitored the various components of SharePoint Server 2013.

Exercise 5: Configuring Network Monitoring

Scenario

To monitor the network infrastructure the .NET web applications rely on, you have to configure network device monitoring in Operations Manager. Configuring monitoring includes discovering the network devices and using the views that are available to monitor the performance and availability of the network devices.

The main tasks for this exercise are as follows:

1. Configure IP addresses on LON-AP2
2. Install the SNMP Device Simulator
3. Configure the SNMP Device Simulator
4. Discover the network devices
5. Simulate a network device failure
6. View the network device Failure alerts in Operations Manager

► Task 1: Configure IP addresses on LON-AP2

1. To perform this task, use the computer and the tool information in the following table.

Location	Value
Computer	LON-AP2
Tool	Network and Sharing Center
Location	Control Panel
Adapter	Local Area Connection 2

2. Edit the **Advance TCP/IP Settings** of the **Local Area Connection 2** adapter and add the following IP addresses to the **Internet Protocol Version 4 (TCP/IPv4)** properties:

- 10.10.0.35
- 10.10.0.36
- 10.10.0.37
- Use a **Subnet Mask** of **255.0.0.0** for all IP addresses

► Task 2: Install the SNMP Device Simulator

1. To perform this task, use the computer and the tool information in the following table.

Location	Value
Computer	LON-AP2
Tool	Setup.exe
Location	C:\Jalasoft\SNMPDeviceSimulator5.0\SNMP Device Simulator 5.0.304.ORTM

Extract the SNMP Device Simulator software, and then run **Setup.exe** from the location specified in the table in step 1.

2. Install the SNMP Device Simulator by using the following settings (all other settings should remain the default settings):

- Agent Service IP Address: **10.10.0.35**

► Task 3: Configure the SNMP Device Simulator

1. To perform this task, use the computer and the tool information in the following table.

Location	Value
Computer	LON-AP2
Tool	Xian SNMP Device Simulator v5 Console
Option	Simulate Device

2. Open the Xian SNMP Device Simulator v5 console, right-click **10.10.0.35:9090**, and then click **Simulate Device**.
3. Use the Simulate Device wizard to create the network devices in the following table (all other settings should be remain the default settings).

Model	IP Address	SNMP
3Com Switch 3900-24	10.10.0.36	V2
Cisco PIX 520 Firewall	10.10.0.37	V2

4. Close the Xian SNMP Device Simulator v5 console, and then log off LON-AP2.

► Task 4: Discover the network devices

1. To perform this task, use the computer and the tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration\Network Management
View	Discovery Rule

2. Use the Discover Network Devices task to run the Network Devices Discovery Wizard, and use the following settings (all other settings should remain as the default settings):
 - Name: **Contoso**
 - Available Servers: **LON-MS1.CONTOSO.COM**
 - Discovery Method: **Explicit**
 - Default Accounts: **Create a new account:**
 - a. Display Name: **Contoso**

- b. Credentials: **public**
- Devices: **Add a device:**
 - a. Name or IP Address: **3Com-3900-24**
 - b. Schedule Discovery: **Run the discovery manually**
- 3. Make sure that the **Run the network discovery rule after the wizard is closed** option is selected.
- 4. Finish the wizard, and then update the view until the Last Discovered column changes from **0** to **1**.
- 5. Under **Network Management**, click **Network Devices**, and then confirm the network devices are discovered.
- 6. Edit the **Contoso** discovery rule and replace **3Com-3900-24** with **CiscoPix-520** and complete the wizard and wait for the network device to be discovered.
- 7. In the **Monitoring** pane, in the **Network Monitoring** folder, review the network devices that are discovered.



Note: It can take up to five minutes for the network devices to be discovered.

► Task 5: Simulate a network device failure

1. To perform this task, use the computer and the tool information in the following table.

Location	Value
Computer	LON-AP2
Tool	Control Panel
Icon	Network and Sharing Center
Edit properties of	Local Area Connection 2

2. Edit the properties of **Internet Protocol Version 4 (TCP/IPv4)**. In the **Advanced TCP/IP Settings** section, remove the **10.10.0.36** IP address, and then save the changes.

► Task 6: View the network device Failure alerts in Operations Manager

1. To perform this task, use the computer and the tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Active Alerts

2. View the Active Alerts view until the **Network Device is Not Responding** alert is generated.



Note: It can take about five minutes for the alert to appear.

3. On the **General** tab of the alert view, the **Alert Description** shows that the **10.10.0.36** device is not responding.
4. From the **Network Monitoring** folder, open the **Network Devices** view, and then notice that the **SuperStack 3900-24** device is in a critical health state.
5. Open the Network Summary Dashboard view, and then select any critical node.
6. From the **Tasks** pane, click **Network Node Dashboard**.
7. View the details in the **Network Node Dashboard**.
8. On LON-AP2, add the **10.10.0.36** IP address back into the **Advanced TCP/IP Settings of the Internet Protocol Version 4 (TCP/IPv4)** settings in **Local Area Connection 2**.
9. After about five minutes, confirm that the **SuperStack 3900-24** device is displayed as healthy again in the Operations console.

Results: After this exercise, you should have configured Network Discovery Rules to discover the network devices that are being simulated on LON-AP2. You should also have simulated a network device failure by removing the IP address details for one of the network devices, and viewed the alert details that Operations Manager generates.

Exercise 6: Configuring Integration Between Operations Manager and Virtual Machine Manager

Scenario

To monitor Virtual Machine Manager and enable Operations Manager to start PRO Tips, you must configure integration between Operations Manager and Virtual Machine Manager. Integration is also required to use the System Center Management Pack for VMM Fabric Dashboard 2012 R2 to monitor the fabric resources in Virtual Machine Manager.

The main tasks for this exercise are as follows:

1. Install an Operations Manager agent on the Virtual Machine Manager server and the Hyper-V host
2. Enable Agent Proxying
3. Install the Operations console on the Virtual Machine Manager server
4. Configure the Operations Manager connection in Virtual Machine Manager
5. Confirm Virtual Machine Manager monitoring

► Task 1: Install an Operations Manager agent on the Virtual Machine Manager server and the Hyper-V host

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
Action	Discovery Wizard

2. Install an agent onto **LON-SC1**, **LON-HOST1** and **LON-HOST2** with the following settings (all other settings should remain the default settings):

- Management Server: **LON-MS1**
- Administrator Account: **Contoso\Administrator**

 **Note:** If the host computer names are different than listed above, substitute LON-HOST1 and LON-HOST2 with the host computer names as configured in the lab environment.

► Task 2: Enable Agent Proxying

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Device Management\Agent Managed

2. Edit the properties of **LON-SC1**, **LON-HOST1** and **LON-HOST2** and from the **Security** tab enable the **Allow this agent to act as a proxy and discover managed objects on other computers** option.

► Task 3: Install the Operations console on the Virtual Machine Manager server

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-SC1
Tool	Setup.exe
Location	\LON-DC1\Media\SCOM2012R2

2. In the **\LON-DC1\Media\SCOM2012R2** folder, use **Setup** to install the Operations console on **LON-SC1**.
3. Open the Operations console, and then connect to **LON-MS1**.

► Task 4: Configure the Operations Manager connection in Virtual Machine Manager

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-SC1
Tool	Virtual Machine Manager Console
Pane	Settings\System Center Settings

Location	Value
Setting	Operations Manager Server

2. Use the Add Operations Manager wizard to configure the Operations Manager connector to Virtual Machine Manager by using the following settings (leave all other default settings):

- Connection To Operations Manager\Server name: **LON-MS1**
- Connection To Operations Manager\Run As Account: **Administrator**
- Connection To VMM\User name: **Contoso\Administrator**
- Connection To VMM>Password: **Pa\$\$w0rd**

3. Wait for the **New Operations Manager connection** job to complete.

 **Note:** It can take up to 15 minutes for the **New Operations Manager connection** job to complete.

4. From the **VMs and Services** pane edit the properties of the **LON-DC1** virtual machine, then from the **General** tab use the **Cloud** drop-down list to select the **Contoso** cloud.

► Task 5: Confirm Virtual Machine Manager monitoring

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Microsoft System Center Virtual Machine Manager Views Microsoft System Center Virtual Machine Manager

2. Open the following views, and confirm the Virtual Machine Manager components have been discovered and are being monitored by Operations Manager:

- Managed Resources\Host Health
- Managed Resources\Virtual Machine Health
- Managed Resources\Virtual Machine Manager Server Health
- Microsoft System Center Virtual Machine Manager Diagram Views\ Diagram View for LON2DSC1

 **Note:** It can take up to 15 minutes for all Virtual Machine Manager resources to be discovered in Operations Manager.

Results: After this exercise, you should have configured integration between Operations Manager and Virtual Machine Manager.

Exercise 7: Using the System Center Management Pack for VMM Fabric Dashboard 2012 R2

Scenario

To effectively monitor the Virtual Machine Manager fabric resources, you must use the System Center Management Pack for VMM Fabric Dashboard 2012 R2. This will enable additional views in the Operations console, such as the Fabric Health Dashboard, which you can use to monitor the health and availability of the Virtual Machine Manager fabric.

The main task for this exercise is as follows:

1. Confirm the Virtual Machine Manager fabric is being monitored

► Task 1: Confirm the Virtual Machine Manager fabric is being monitored

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Microsoft System Center Virtual Machine Manager\Cloud Health Dashboard\Cloud Health

2. Open the **Cloud Health** view and confirm the private clouds have been discovered and are being monitored by Operations Manager.

 **Note:** If a message stating The **Dashboard view has been deleted or no longer exists** appears then close the Operations console and then re-open it.

3. Select **Contoso** Private Cloud and then from the **Tasks** pane use the **Fabric Health Dashboard** task to open the **Fabric Health Dashboard**.
4. Review the **Fabric Health Dashboard**.

 **Note:** The **Fabric Health Dashboard** will not display any data until all VMM resources have been discovered but you can review the data that will be displayed when discovery has completed.

5. Expand **Microsoft System Center Virtual Machine Manager Views**, and then open the **Diagram View for LON2DSC1**
6. Expand **Managed Resources**, and then review the Virtual Machine Manager Fabric resources that are being monitored.

Results: After this exercise, you should have used the System Center Management Pack for VMM Fabric Dashboard 2012 R2 to confirm that the relevant Virtual Machine Manager fabric resources are discovered and monitored in Operations Manager.

Question: What must you install on the Virtual Machine Manager server when configuring integration between Operations Manager and Virtual Machine Manager?

Question: After installing the System Center Management Pack for SharePoint Server 2013, what action should you perform in the Operations console so that the SharePoint components can be discovered and monitored?

Module Review and Takeaways



Best Practice: As a best practice, it is recommended that you install one or only a small number of Management Packs and wait 24 hours before you install other Management Packs. During this time, monitor the alerts that the Management Pack generates. By installing Management Packs gradually, you can fine-tune the Management Pack with overrides that are customized for your environment before you install another Management Pack.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
After installing and configuring the System Center Management Pack for SharePoint Server 2013, you might notice that not all servers in the SharePoint farm are discovered and monitored.	

Review Question(s)

Question: You must create a task that will be made available to operators in the Operations console. The task will be used to open a log viewer that connects to the selected computer and opens the latest error log for an in-house application. The log viewer application is installed on the same computer as the Operations console. What type of task should you create for this?

Real-world Issues and Scenarios

In scenarios where the default action account of an agent does not have sufficient permissions required by a Management Pack, you can use Run As accounts and Run As profiles to provide credentials to the workflows within a Management Pack to allow them to run with the required permissions. For more information about Run As accounts and Run As profiles, visit this link:

<http://go.microsoft.com/fwlink/?LinkId=391270>

Tools

If you need to test Operations Managers network monitoring capabilities but do not have any network devices in your test environment, you can use a network device simulator such as the Xian SNMP Device Simulator from Jalasoft. Using this free simulator, you can create a number of virtual network devices that Operations Manager can discover and monitor. For more information about the Xian SNMP Device Simulator, including download instructions, visit this link:

<http://go.microsoft.com/fwlink/?LinkId=391271>

Module 5

Application Performance Monitoring

Contents:

Module Overview	5-1
Lesson 1: Application Performance Monitoring	5-2
Lesson 2: Using IntelliTrace	5-18
Lesson 3: Team Foundation Server Integration	5-23
Lab: Monitoring .NET Framework Applications	5-26
Module Review and Takeaways	5-38

Module Overview

Most organizations use the Microsoft .NET Framework to build custom applications, such applications as for intranet websites. Because Management Packs for custom applications are not available, you should understand how application performance monitoring (APM) is configured in Microsoft System Center 2012 R2 Operations Manager. APM provides extensive monitoring for applications based on .NET and Java and includes both server-side and client-side monitoring.

In addition to understanding how to monitor .NET applications directly by using Operations Manager, it is important that you understand how APM can be used with the IntelliTrace Collector for Microsoft Visual Studio to gather full application profiling traces. With System Center 2012, you can also integrate Operations Manager with Team Foundation Server (TFS). You must understand how this integration is configured so that Operations Manager can be used to synchronize alerts with work items in TFS.

Objectives

After completing this module, students will be able to:

- Configure application performance monitoring (APM).
- Configure Microsoft IntelliTrace with APM to debug .NET applications.
- Integrate Microsoft System Center 2012 R2 Operations Manager with Team Foundation Server (TFS).

Lesson 1

Application Performance Monitoring

It is often challenging for IT professionals to understand how to monitor custom .NET applications. This is largely because few custom applications are developed effectively for monitoring. It can be very difficult to identify issues that originate in the code base. Development teams can incorrectly assume an infrastructure issue is the cause, and infrastructure teams can incorrectly attribute an issue to the application.

APM was developed to bridge the gap between IT professionals and developers by providing deep code-level monitoring of .NET applications. With System Center 2012 R2 Operations Manager, this monitoring has been extended to Java-based applications.

When addressing performance issues in .NET-based and Java-based applications, you need to understand how APM can be configured to provide deep monitoring of the application so that you can identify where the issue is. APM also provides insight into the performance impact for end-users.

Lesson Objectives

After completing this lesson, students will be able to:

- Identify the prerequisites for monitoring .NET applications.
- Use the .NET Application Performance Monitoring template.
- Configure advanced client-side monitoring.
- Configure advanced server-side monitoring.
- Use the Application Diagnostics console.
- Use the Application Advisor console.
- Configure Operations Manager to monitor Java EE applications.

Prerequisites for monitoring .NET Applications

APM can monitor ASP.NET and Windows Communication Foundation (WCF) applications that are hosted on either Microsoft Internet Information Services (IIS) 7.0 or IIS 8.0. Additionally, Windows Services that are written using the .NET Framework can also be monitored by APM.

Before you monitor a .NET Framework application by using Operations Manager, you must understand the basic components included in the application so that you can customize monitoring of the application, including monitoring thresholds. These thresholds are used to determine when the application is performing poorly. You usually collect this information from the application owner or the software developer, or from both. To help you obtain the information required to monitor the application effectively, consider the following questions:

- What are the names of the applications that require monitoring?
- Which computers host the applications?

Before monitoring .NET applications, you should:

1. Understand the basic components of the application

- ?
- What are the names of the applications that require monitoring?
- ?
- Which computers host the applications?
- ?
- Is performance event monitoring required?
- ?
- Is exception event monitoring required?
- ?
- What thresholds signify a performance issue with the application?
- ?
- Are both server-side and client-side monitoring required?

2. Import the related Management Packs

- Is performance event monitoring required?
- Is exception event monitoring required?
- What thresholds signify a performance issue with the application?
- Are both server-side and client-side monitoring required?

You should also make sure that an Operations Manager agent is deployed to the computers that are hosting the .NET Framework application. When you install the Operations Manager agent, an APM agent is also installed. The APM agent runs as a service named System Center Management APM. By default, this service is disabled until it is required.

Additionally, the following Management Packs must be installed in order to discover the applications:

- Windows Server 2008 Internet Information Services 7.0 (for IIS 7.0 applications)
- Microsoft System Center APM Web IIS 7 (for IIS 7.0 applications)
- Windows Server 2012 Internet Information Services 8.0 (for IIS 8.0 applications)
- Microsoft System Center APM Web IIS 8 (for IIS 8.0 applications)

To use the Application Advisor and Application Diagnostics console to troubleshoot application performance issues, the Operations Manager Web console must also be deployed.

After the Operations Manager agent is deployed to the computers that host the .NET Framework application, and the related Management Packs are imported, Operations Manager automatically discovers the .NET Framework applications. To view these .NET Framework applications, use the ASP.NET Web Application Inventory view. This view is located in the Application Monitoring\NET Monitoring folder. The folder can be accessed from the Monitoring pane of the Operations console.

If client-side monitoring of the application is required, the Check Client-Side Monitoring Compatibility task should be run against the .NET Framework application. The task becomes available in the Operations console, in the ASP.NET Application Endpoint Tasks section of the Tasks pane, when the .NET Framework application is selected in the ASP.NET Web Application Inventory view.

When the task is run, the Task Output displays any incompatible pages for the application. This output includes an explanation of why the pages are incompatible and the possible resolutions that can be applied to correct or reduce the incompatibility. Also, the related pages are listed so that they can be excluded from client-side monitoring when it is configured.

 **Note:** If the Windows Services that are running in the .NET Framework application must be monitored, those services must be monitored by using the Windows Services template before the services can be added as part of an APM monitor.

More information about what do to before you begin monitoring .NET Framework applications can be found on the following link.

 **Before You Begin Monitoring .NET Applications**

<http://go.microsoft.com/fwlink/?LinkId=321880>

Information about how to mask or avoid the collection of sensitive data can be found on the following link.

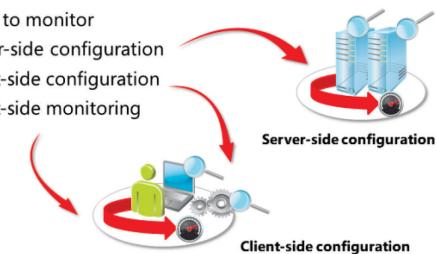
**Working with Sensitive Data for .NET Applications**<http://go.microsoft.com/fwlink/?LinkId=321897>

Guidelines for Using the .NET Application Performance Monitoring Template

After Operations Manager has discovered the .NET Framework application, monitoring of the application is configured by using the Add Monitoring Wizard with the .NET Application Performance Monitoring template. Both server-side and client-side monitoring can be configured by using this template. However, client-side monitoring cannot be configured without server-side monitoring. The following table provides a description of each page of the Add Monitoring Wizard that is used with the .NET application Performance Monitoring template.

To configure monitoring of a .NET application, configure the .NET Application Performance Monitoring Management Pack template and include:

- What to monitor
- Server-side configuration
- Client-side configuration
- Client-side monitoring



Client-side configuration

Add Monitoring Wizard page	Details
General Properties	On this page, you specify a descriptive name for the monitor such as DinnerNow – Production. You also specify the Management Pack in which the monitor should be saved. It is recommended that you create a new Management Pack for any new .NET Framework application that will be monitored. This enables the Management Pack to be exported and backed up easily, and also allows for the Management Pack to be imported into other Management Groups such as development or test.
What to Monitor	On this page, you add the application components that should be included in this monitor. You first select the component type, such as Web Applications And Services or Windows Services. Then, you search the components that Operations Manager discovers and add the related component that should be included as part of this monitor. You can also add an environment tag, such as Production or Staging. This is useful because additional monitors can be created for different environments. Operations Manager creates views in the Operations console that relate to the environment tag. Additionally, you can create or select a Targeted group that is used to scope which computers the monitors should be applied to.
Server-Side Configuration	On this page, you configure basic monitoring of the application. This includes enabling performance and exception event alerts and setting the performance event threshold in milliseconds. By default, this is set to 15000 milliseconds.
Server-Side Configuration (Advanced Settings)	By clicking Advanced Settings on the Server-Side Configuration page, you can customize monitoring for the application from the server side. This is discussed in the topic "Advanced Server-Side Monitoring" later in this lesson.
	<p> Note: If the <i>Enable Additional Configuration Options For Server-Side And Client-Side Monitoring</i> check box is selected on the Server-Side Configuration page, the following three additional pages are added to the wizard:</p>

Add Monitoring Wizard page	Details
	<ul style="list-style-type: none"> • Server-Side Customization • Client-Side Configuration • Enable Client-Side Monitoring
Server-Side Customization	On this page, you can customize monitoring for the server-side aspect of the application. This includes enabling application failure alerts, changing monitor thresholds, and adding a specific transaction to the monitor. This is discussed in detail in the topic "Advanced Server-Side Monitoring" later in this lesson.
Client-Side Configuration	On this page, you configure the client-side monitoring of the application, including performance and exception event alerts, the page load, Ajax and WCF thresholds, and the client IP address filter. The client IP address filter is used to filter IP addresses that should be included or omitted in client-side monitoring. By default, only local host IP addresses are monitored.
Client-Side Configuration – (Advanced Settings)	By clicking the Advanced Settings button on the Client-Side Configuration page, you can customize the monitoring for the application from the client side. This is discussed in the topic "Advanced Client-Side Monitoring" later in this lesson.
Enable Client-Side Monitoring	On this page, you can either enable or disable client-side monitoring for web applications. By enabling this option, JavaScript scripts are added to each managed web application, which are then used to monitor the application from the client-side. By clicking the Customize button on this page, you can also configure additional monitoring, such as load balancer settings, excluded pages, and data items that should be included in data collection, such as images and scripts. This is discussed in the topic "Advanced Client-Side Monitoring" later in this lesson.
Summary	On the Summary page, a summary of the options that are selected during the wizard is displayed. You can use these options to go back through the wizard and make changes, if necessary. A warning message might also be displayed here noting that IIS might have to be restarted. Restarting IIS is required to add extensions to the application so that APM can monitor the application.

In most cases in which changes to the monitoring of an application are made, IIS will have to be restarted. The IIS Restart/Recycle Required view in the Operations Manager\APM Agent Details folder of the Monitoring pane can be used to determine on which computers IIS must be restarted. The view contains an IIS Restart and an IIS Recycle section. By selecting a computer in either section, the Restart Internet Information Services and Recycle Application Pools tasks become available. These tasks help by performing the operations remotely so that you don't have to log on to the computer and start Internet Information Services Manager.

After basic monitoring is applied, several views are created in the .NET Monitoring folder in the Monitoring pane in the Operations Console. The following table provides a description of the views.

APM .NET Monitoring view	Description
Active Alerts	Displays all .NET Framework Application Component alerts that are not resolved.

APM .NET Monitoring view	Description
Monitored Applications	A health state view that displays the health state of each monitored application.
<i>ApplicationName\Active Alerts</i>	A folder is created by using the name of the application that is specified when you use the Add Monitoring Wizard, such as DinnerNow – Production. The Active Alerts view displays all .NET Framework application component alerts that are not resolved for the application.
<i>ApplicationName</i>	A health state view that displays the health state of the monitored application.
<i>ApplicationName\All Performance Data</i>	Performance counters that are collected for the application are displayed on this page. Objects can be selected and added to a graph that can then be used to determine how the application has performed during selected dates and times.
<i>ApplicationName\Overall Component Health</i>	This view contains an Application State pane that displays the health state of the monitored components of the application, and an Active Alerts pane that displays alerts that are not resolved for the application.
<i>ApplicationName\{Client}\ All Performance Data</i>	If client-side monitoring is enabled, a separate folder is created for client monitoring. The All Performance Data view displays performance counters that are collected from the client-side.
<i>ApplicationName\{Client}\Overall Component Health</i>	This view contains an Application State pane that displays the health state of the monitored components, and an Active Alerts pane that displays alerts that are not resolved for the application from the client-side.



Note: In most cases, the Details View that can be found in the bottom pane of the selected view displays useful information that relates to the view. For example, the Detail view for the Overall Component Health view displays the settings for the application that is being monitored. This includes the % Performance Events/sec threshold and the % Exception Events/sec threshold. These can be used to match alerts that are generated with the current thresholds that are set, and will help if the settings have to be changed.

More information about how to configure monitoring for the .NET Framework applications can be found on the following link:

How to Configure Monitoring for .NET Applications

<http://go.microsoft.com/fwlink/?LinkId=321881>

Advanced Client-Side Monitoring

After you use the Add Monitoring Wizard to apply base monitoring of the .NET Framework application, you can edit the monitor from the .NET Application Performance Monitoring view. This view is located in the Management Packs templates, in the Authoring pane of the Operations console.

On the Client-Side Monitoring tab in the Properties window, you can use the Customize button to configure several advanced options. The following table provides a description of some common options that are configured.

Advanced client-side monitoring includes:

- Page load thresholds
- Sampling
- Client IP address filter
- Monitors
- Data collection
- Load balancer settings
- Excluded pages
- Transactions
- Monitored servers

Client-Side Monitoring option	Description
Page Load Threshold (ms)	This setting determines the expected response time in which the page should load. The default is 15000 milliseconds (ms).
Sampling	By default, all incoming requests are monitored from clients. You can set a percentage of incoming requests that should be monitored. This helps when clients originate from the same location, because the response time for these clients is usually the same or similar. You can reduce the percentage to only sample 50 percent of incoming requests, for example.
Client IP Address Filter	By setting a client IP address filter, you can filter specific subnets that you do not want to include in client-side monitoring. For example, you can have several internal client computers that do not use the application. Adding a filter that includes the network that these client computers are connected to will result in the client computers not being included in the monitored scope. This helps improve performance of APM and reduces space that is required in the Operations Manager databases where monitored data is stored.
Monitors	You can customize the percentage threshold of exception and performance events that should be accepted over a specific time interval. By default, the % Exception Event/sec threshold is 15 percent over a five-minute interval. This means that if more than 15 percent of all transactions that are monitored result in an exception, an alert will be generated. Establishing this threshold helps, because an alert is not generated for every exception, which would result in a flood of alerts. Instead, an alert is generated when exceptions are at a sustained level, which indicates there is an issue. Similar monitors are included for Performance Events and Average Request Time.
Data Collection	Several data collection items exist that can be included in client-side monitoring. These include Images, Scripts, Cascading Style Sheets (CSS), Global Variables, and the Exception Stack. When the items are enabled, they are displayed in the Operations console views. These items can help determine page load issues when transactions are run. It is recommended that the Global Variables and Exception Stack data items be used only when the application is configured for HTTPS, because these data items send application data to the monitored server, and this data could include sensitive data.

Client-Side Monitoring option	Description
Load Balancer Settings	When load balancers are used from the client-side, the client's real IP address is masked by the load balancers' virtual IP address. This means that APM cannot determine the real IP address of the client. By enabling the related load balancer on this page, you enable the HTTP request header to be captured. This header includes the client's real IP address. Support for several load balancers, such as AKAMAI, Cisco/NAT, F5, and RFC, is included.
Excluded Pages	You can exclude specific pages from being monitored by using this option. You can use this for pages in the application that are under maintenance and should not be included. Additionally, you might have pages that are incompatible based on the Check Client-Side Monitoring Compatibility task discussed earlier. These pages would be excluded here.
Transactions	You can add specific transactions (or pages) that should be monitored from the client. This helps when an application uses pages that might not be directly accessed by an end-user, although they are still important to the application that is being monitored. Additionally, each transaction can be configured by using its own performance and exception event threshold. This helps when certain pages of an application take longer than other pages to process. The transactions for these pages can be added here with different thresholds that are more significant to the application.
Monitored Servers	When monitoring a .NET Framework application in multiple environments, you can use the Monitored Servers option to target specific groups of servers on which the application runs, such as Production or Development. This controls to which servers the APM configuration is distributed.

Advanced Server-Side Monitoring

When you configure the server-side monitoring of an application in APM, you can use the Advanced Settings button to configure several settings. The following table provides a description of some common settings.

Advanced server-side monitoring includes configuring settings for the following:

- Events
- Performance events
- Namespaces
- Methods
- Exception events
- Exception tracking
- Critical exceptions
- Monitors
- Monitored servers

Advanced server-side monitoring setting	Description
Event Monitoring	Using this setting, you can enable performance and exception event alerts that relate to a defined percentage of alerts over a specific time period.
Performance Event Monitoring	Using this setting, you can configure the performance event threshold to determine the time in milliseconds that the server is expected to generate the page. The default is 15000 milliseconds. Additionally, you can configure the Sensitivity threshold. This threshold determines the permitted gap between exception events that are included in monitoring thresholds.
Set Namespaces	Use this option to add classes and methods to the application that APM will monitor for additional timing information. When you view an exception event, this data, when collected, displays a detailed execution tree, including details of the affected items, in the Application Diagnostics console. Namespaces are automatically included for known .NET exceptions, such as IIS. For this option, you add the namespace that is specific to the application that APM has no knowledge of.
Set Methods	Use this option to collect additional parameter data that relates to namespace exception events to help you troubleshoot exception events. Frequently, it can be difficult to determine where in an application's code an exception occurs. By adding parameters, developers can collect and use the related data to help pinpoint a path of issues in the application.
Exception Event Monitoring	With the settings here you can select whether APM should collect all exceptions or critical exceptions only. You can also select to monitor security alerts, such as a logon failure, or connectivity alerts, such as database connectivity. You can also monitor application failure alerts, such as a missing or unregistered DLL. Typically, you enable these settings first so that you can understand how the application is performing. This process is known as <i>baselining</i> . As soon as a baseline is taken, you adjust these alerts settings based on the results from the baseline.
Exception Tracking	By adding exception tracking, you can include additional exception variables or parameters that should be collected when an exception occurs.
Critical Exceptions	By adding critical exceptions, you can define exception functions that generate events and perform error handling.
Monitors	You can customize the percentage threshold of exception and performance events that should be accepted over a specific time interval.

Advanced server-side monitoring setting	Description
	Refer to Monitors in the Advanced Client-Side Monitoring section for more information on this.
Monitored Servers	You can add or select a computer group here to restrict the servers included in server-side monitoring.

Guidelines for Using the Application Diagnostics Console

The Application Diagnostics console is an additional console dedicated to managing events from monitored .NET Framework applications in Operations Manager. Its main purpose provides a method of pinpointing the source of application failures and performance issues in the .NET Framework applications.

The Application Diagnostics console is available only when the Operations Manager Web console is deployed. You can open the console in two ways: by browsing to it directly, or by clicking a link provided in the Alert Description section of an alert generated by APM in the Operations console. The URL that is used to connect to the console is <http://WebConsoleServerName/AppDiagnostics>. You must be a member of the Application Monitoring Operator or Administrator user role in Operations Manager to use the Application Diagnostics or Application Advisor consoles.

When you view events in the Application Diagnostics console, you can group events into problem groups. Because events from the same source are grouped, you can pinpoint application issues much more quickly and easily.

The Application Diagnostics console displays two main types of events: application performance events and the events related to application failures and errors. Failure and error events can also be further divided into categories such as connectivity, security, and failure issues.

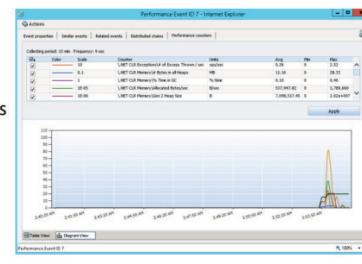
When you select an event such as a performance event, the event details are displayed and distributed into five main tabs. A description of the five tabs follows.

Event Properties

The Event Properties tab includes details such as the event class, component, source, and status. The computer that generated the event and the event class, such as Performance, is also displayed here. Details included in this section are context-sensitive, so depending on the type of event, the details included will differ. For example, a server-side performance-related event might include a stack trace of a method that is implemented on a server. A client-side performance-related event might include details about how long it takes the client to download and display a webpage. By expanding the stack, you can view the order in which the events occurred. You can change the view to Resource Group view or Execution Tree view to help you investigate the many calls made to the application and determine where in the application the issue occurred.

The Application Diagnostics console manages events from monitored .NET applications and includes:

- Event properties
- Similar events
- Related events
- Distribution chains
- Performance counters



Similar Events

The Similar Events tab is used to view events from the same source during a specific time period. This view shows how frequently an event occurs between two time periods. You can use this to match events with application performance and failure issues to help identify trends. Additionally, events can be filtered by Problem or Heaviest Resource, and also grouped by Heaviest Resource Call. This group shows events that are close to breaching a threshold.

Related Events

The Related Events tab is useful in correlating events from the same resource that occurred in a set time frame. For example, you can specify a period of one hour, and all related events from the same source will be displayed. You can then select any of the returned events and view the details as you would view them for any other event.

Distribution Chains

The Distribution Chains tab shows the components that are involved in the event. This includes how the events relate to one another. The last event in the chain is the event that breached the threshold. By clicking this event, you can investigate the event details.

Performance Counters

The Performance Counters tab displays performance counters for the system before, during, and after the event. This view shows how the system performed before the event occurred and how the event affected the system during and after the event. Performance counters such as % Processor Time, Avg. Request Time, and Exception Events/Sec are included. The performance counters can help determine how the system and the application are performing at the time of the event. Here, details can be viewed in a graph or in a Table View. You can use this when specific values for performance counters must be viewed.

More information about how to work with the Application Diagnostics console can be found on the following link:

Working with the Application Diagnostics Console

<http://go.microsoft.com/fwlink/?LinkId=321882>

Guidelines for Using the Application Advisor Console

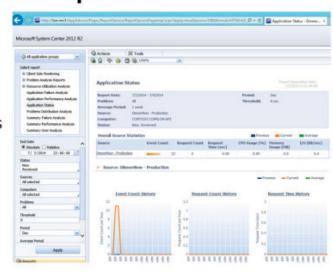
You use the Application Advisor console to view and prioritize alerts from monitored .NET Framework applications in the environment, and to identify applications that are causing the most alerts in the environment. By identifying these applications, you can better focus your initial investigations.

As with the Application Diagnostics console, the Applications Advisor console is available only when the Operations Manager Web console is installed. It can be opened directly in the following two ways:

- By browsing to <http://<WebConsoleServerName>/AppAdvisor>
- By clicking the Advisor link in the Application Diagnostics console

The Application Advisor console can display and help prioritize alerts from monitored .NET applications and includes reports for:

- Client-side monitoring
- Problem analysis
- Application analysis
- Resource utilization analysis
- Performance summary



Additionally, the Application Advisor console requires SQL Server Reporting Services, which is already available when Operations Manager Reporting is deployed.

The Application Advisor console includes several reports that can be used to view the health of a monitored .NET Framework application. Reports are divided into categories, such as Client-Side Monitoring, Problem Analysis Reports, and Resource Utilization Analysis. Several Summary reports also exist, including the Summary Failure Analysis and Summary Performance Analysis reports, which you can use to show an at-a-glance view of the .NET Framework application's health.

Running Reports in the Application Advisor Console

Before you run a report in the Application Advisor console, you first select the application group to which the report will be scoped. You create Application groups in the Application Diagnostics console. Application Groups provide a method to group .NET Framework Applications for event analysis.

After you select the Application group, you must select the report that you want to run, such as an Application Analysis report. Before you run the report, you can apply several filters to the report to help filter the report to meet your requirements. For example, you can select a relative or absolute start and end date for the report. The Absolute option lets you specify a specific date and time, whereas for the Relative option, you can specify a date, such as yesterday or the previous month. You can also filter the report, depending on a specific computer or issue type such as Critical. The list of filters available varies, depending on the report selected.

To run a report and then view it in the Details pane, click the Apply button.

Reports can also be scheduled to run on a timed basis and then emailed to staff members who want them. Reports can be exported to several different formats such as .pdf, .xls, and .tiff.

The following table provides a description of some of the reports that are available in the Application Advisor console.

Application Advisor report	Description
Client-Side Monitoring\Application Analysis	This report provides an overview of the performance and activity of the selected application. It also includes the exception statistics. It displays the counts for the top 10 exception events of an application. This information helps obtain an overall view of an application's health from the client-side.
Problem Analysis Reports\Day of Week Utilization	This report is used to view application activity trends and application resource utilization trends over a specific time period. This information can be used to determine the periods in which the application is used most frequently.
Resource Utilization Analysis\Computer Application Load Analysis	This report is used to provide an analysis of servers based on processed requests. It analyzes the load on the servers and includes CPU, Memory and IO utilization. This information can then be used to determine the most affected servers and help with capacity planning for application resources.
Summary Failure Analysis	This report can be used to show a breakdown of issues by application. It shows the top five issues for each application and shows the issues as a percentage of the total issues. Because this report highlights the most common issues in an application, you can use this report to decide where you want to focus resources to troubleshoot the applications issues that occur.
Summary Performance Analysis	This report can shows a breakdown of performance violations for each application. It displays the top five performance issues for each application and shows the issues as a percentage of the

Application Advisor report	Description
	total performance issues that occur.

More information about how to prioritize alerts by using Application Advisor can be found at the following link:

Prioritizing Alerts by Using Application Advisor

<http://go.microsoft.com/fwlink/?LinkId=321883>

Guidelines for Monitoring Java EE Applications with Operations Manager

With the release of System Center 2012, Operations Manager now provides Management Packs for Java Enterprise Edition (JEE). These Management Packs include the automatic discovery of Java-based applications. These applications are installed in the most frequently used JEE application servers. These servers include Apache Tomcat, Red Hat JBoss, IBM WebSphere, and Oracle WebLogic. Operations Manager can monitor these applications on both Windows-based and UNIX/Linux-based deployments. The following table provides a description of the supported operating systems.

Operations Manager supports monitoring of the following Java EE applications:

- Apache Tomcat
- Red Hat JBoss
- IBM WebSphere
- Oracle WebLogic

• Monitoring capabilities include:

- Process availability health
- JMX store configuration health
- Percentage of virtual machine memory utilized
- Individual Java application availability health
- Garbage collection rate performance monitor (per collector)
- Garbage collection time performance monitor (per collector)

JEE application server (versions)	Supported operating system
Apache Tomcat (5.5, 6.x, 7.x)	RHEL, SLES, Windows
Red Hat JBoss (4.2, 5.1, 6.x)	RHEL, SLES, Windows
IBM WebSphere (6.1, 7.x)	RHEL, SLES, AIX, Windows
Oracle WebLogic (10gR3, 11gR1)	RHEL, SLES, Solaris, Windows

After a Java application is discovered by the JEE Management Packs, Operations Manager can collect any exposed probes. These probes are known as *managed beans*, or *MBeans*. The probes channel the application by using Java Management Extension (JMX), which is a standard management interface for Java. Operations Manager achieves this monitoring by using a Java servlet called *BeanSpy*. Microsoft developed BeanSpy, and BeanSpy is open sourced.

Because BeanSpy is open sourced, and the source code is available to download from GitHub, monitoring for the JEE Management Packs and BeanSpy can be extended. Extension can result from continued development in the Java community or from companies that need and develop additional functionality.

Configuring the JEE Management Packs

After the Linux/UNIX agent is installed, and the server is discovered by Operations Manager, the JEE Management Packs must be installed and configured. You do this by downloading the installation package and documentation from the Microsoft Download Center. You must execute the MSI install executable, and then import the extracted Management Packs that are required to monitor the JEE platform in the environment. There are Management Packs for each JEE application server. It is

recommended that you install only the Management Packs that are associated with the platform in the IT environment.

More information about how to download the System Center 2012 - Operations Manager Component Add-On can be found at the following link:

 **System Center 2012 - Operations Manager Component Add - On**

<http://go.microsoft.com/fwlink/?LinkId=321884>

After the required Management Packs are installed in Operations Manager, you must configure the JEE monitoring account profile. You do this by using the Create Run As Account wizard in the Administration workspace of the Operations console. Then, you use the account that has the JEE Monitoring Account profile.

After Operations Manager discovers the installation of the JEE application server, BeanSpy should be deployed to the server. This enables the discovery and monitoring of the Java applications that are installed in the application server. You do this by using the Copy BeanSpy and Universal Discovery Files task in the Tasks pane. However, you view the JEE application server instance in the Monitoring pane of the Operations console, under JEE Application Servers Profiles. The BeanSpy components are copied to the %WINDIR%\Temp folder. The Management Pack documentation describes the file that is used for deployment to the JEE application server; the file used depends on the server's configuration. As soon as the file is deployed, it is recommended that you confirm BeanSpy is functional and go to its web service by using a web browser. The following URL format should be used to connect to the web service:

- `http://<FQDN>:<port>/BeanSpy/Stats/Info`
- `http://<FQDN>:<port>/BeanSpy/MBeans?JMXQuery=<JMXQuery>`

Included in the documentation for each JEE Management Pack are example URLs that are specific to the JEE application server being monitored. If the query is successful, the response from the web service should be an XML page that is representative of the MBean that matched the specific query.

To discover the individual applications that are installed on the JEE application server, you must enable Deep Monitoring. You do this by using the Enable Deep Monitoring through HTTP task that is located in the Profiles state view. When the task is executed, a task execution wizard is displayed. The wizard must be executed and allowed to finish. After a short time, the Applications state view will be populated with each Java application that is installed in the JEE application server.

At this point, the applications should be collecting both performance and availability metrics. The applications should also be monitoring these metrics against the default thresholds that are set in the Management Pack. One final step for default configuration that an IT professional can complete relates to the following three disabled performance threshold monitors for Java applications:

- Garbage Collection Rate of a Java EE Application Server (for each garbage collector)
- Garbage Collection Time of a Java EE Application Server (for each garbage collector)
- Performance monitor for the Percentage of Virtual Machine Memory Used on a Java EE Application Server

By default, the three optional monitors are disabled because of the different monitoring requirements for each organization and application. Although the JEE Management Pack features can be extended, this extension must be supported by the JEE application through additional instrumentation provided as an MBean, and it must use a Custom Application Monitoring template. Two templates are provided by the JEE Management Packs that enable both additional availability monitoring and performance monitoring. To use these templates, use the Authoring workspace in the Operations console, and then in Management Pack Templates, click JEE Application Availability Monitoring or JEE Application Performance Monitoring.

When you use these templates, an intuitive wizard interface is provided. This interface enables the selection of the Java application target, profile target, MBean target, and health state determination.

Features of the JEE Management Packs

Operations Manager intuitively monitors important availability and performance metrics. These metrics include the following:

- Process availability health
- JMX store configuration health
- Percentage virtual machine memory utilized performance health
- Individual Java application availability health
- Garbage collection rate performance monitor (for each collector)
- Garbage collection time performance monitor (for each collector)

The following rules are provided to collect performance data:

- JVM loaded class count
- JVM total loaded class count change rate
- JVM total unloaded class count change rate
- JVM peak thread count
- JVM current running thread count
- JVM total started thread count change rate
- JVM JIT compiler time change rate
- JVM initial heap memory allocated
- JVM heap memory used
- JVM maximum heap memory committed
- JVM maximum heap memory
- JVM percentage of heap memory used
- JVM object pending finalization (garbage collection)

The following health state views are provided by the Management Pack:

- **Application State.** Provides visibility of State, Application Name, Object Name, and Path
- **Profile State.** Provides visibility of State, Host Name, Profile, Cell, Node, Server, HTTP Port, HTTPS Port, Version, Disk Path, Path
- **Deep Monitored Profile State.** Provides visibility of State, Host Name, Profile, Cell, Node, Server, HTTP Port, HTTPS Port, Version, Path, Protocol, Port, Disk Path

The following performance graph views are provided:

- Class loader
- Heap memory
- Garbage collector
- Threads
- JIT compiler

Demonstration: Configuring Application Performance Monitoring

In this demonstration, you will learn how APM is configured in Operations Manager.

Demonstration Steps

- To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

- Browse to **\LON-DC1\Media\SCOM2012R2\ManagementPacks**, and then copy the **Microsoft.SystemCenter.APM.Web.IIS7.mp** file to the desktop of LON-MS1.
- Open the Operations console and import the **Microsoft.SystemCenterAPM.Web.IIS7.mp** Management Pack.
- To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Authoring
View	Management Packs Templates

- Use the Add Monitoring Wizard to configure the **.NET Application Performance Monitoring** template with the following settings (all other settings should remain as the default settings):
 - Name: **DinnerNow**
 - Management Pack: Create a new Management Pack named **DinnerNow_Demo**
 - What to Monitor: **DinnerNow**
 - Monitoring Scope: **Production**
 - Server-Side Configuration\Performance Event Threshold: **50**
 - Enable additional configuration options for server-side and client-side monitoring
 - Server-side Customization\Customize: **Enable Application Failure Alerts and All Exceptions**
 - % Exception Events/sec exceeds threshold: **1**
 - % Performance Events/sec exceeds threshold: **1**
 - Average Request Time exceeds threshold: **10**
 - Client-side Configuration: **Turn on exception event alerts**
 - Page load threshold (ms): **50**
 - Ajax and WCF threshold (ms): **5**

- Configure client IP address filter: **Remove both filters**
 - Advanced Settings\ Sensitivity threshold (ms): **5**
 - Page load threshold (ms): **5**
 - % Exception Events/sec exceeds threshold: **1**
 - % Performance Events/sec exceeds threshold: **1**
 - Average Request Time exceeds threshold: **10**
 - Enable Client-Side Monitoring: **Enabled**
6. Cancel the wizard before creating the monitor.

Question: You have to monitor a .NET web application on a computer that is running Windows Server 2012. In addition to the operating system and IIS Management Packs, what other Management Pack do you have to install for Operations Manager to discover the .NET Framework application?

Lesson 2

Using IntelliTrace

New in System Center 2012 R2 is the ability of Operations Manager to collect IntelliTrace logs from IIS servers hosting web applications. Collecting these logs provides an additional troubleshooting feature when you are troubleshooting issues with web applications. You can view IntelliTrace logs from exception events generated by APM. When monitoring .NET web applications with APM, it is important to understand how APM can be used with the full functionality of the IntelliTrace Collector for Visual Studio to gather complete application profiling traces. Additionally, when Operations Manager and TFS are integrated, these IntelliTrace logs can be converted to work items in TFS.

Lesson Objectives

After completing this lesson, students will be able to:

- Enable IntelliTrace logging.
- Collect and view IntelliTrace logs.

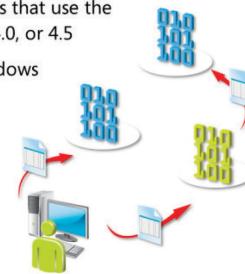
How IntelliTrace Works

Included with the Microsoft Monitoring Agent is the ability to use IntelliTrace to debug applications written in the .NET Framework platform. More specifically, IntelliTrace can be used to debug the following applications:

- Microsoft Visual Basic and Microsoft Visual C# apps that use the .NET Framework 2.0, 3.0, 3.5, 4.0, or 4.5
- ASP.NET, Microsoft Azure, Windows Forms, WCF, Windows Presentation Foundation (WPF), Windows Workflow, SharePoint 2010, SharePoint 2013, and 64-bit apps
- SharePoint applications
- Microsoft Azure apps

IntelliTrace can be used to collect trace debug logs from the following applications:

- Visual Basic and Visual C# apps that use the .NET Framework 2.0, 3.0, 3.5, 4.0, or 4.5
- ASP.NET, Windows Azure, Windows Forms, WCF, WPF, Windows Workflow, SharePoint 2010, SharePoint 2013, and 64-bit apps
- SharePoint applications
- Windows Azure apps



You can use the IntelliTrace feature as a stand-alone debugging tool with the Microsoft Monitoring Agent. However, when the Microsoft Monitoring Agent is connected to a System Center 2012 R2 Operations Manager Management Group, additional features become available. These include:

- Real-time alerting
- Operational reporting
- Centralized management of configuration

Additionally, the IntelliTrace logs that are collected can be attached to alerts in the Operations Console and can also be forwarded as Work Items in TFS. TFS integration is covered in greater detail later in this module.

Enabling IntelliTrace Debugging Locally (Without a Connected Microsoft Monitoring Agent)

After you install the Microsoft Monitoring Agent on a computer hosting a .NET application, you can perform the following steps to enable IntelliTrace log collection:

1. Start Windows PowerShell as a local administrator.
2. Use the **Get-WebSite** or **Get-WebApplication** cmdlets to determine the web application name to be debugged.
3. Use the **Start-WebApplicationMonitoring** cmdlet to start debugging.
4. Use the **Stop-WebApplicationMonitoring** cmdlet to stop debugging.

When you use the **Start-WebApplicationMonitoring** cmdlet to start debugging, you are prompted for the following additional information:

- **Name.** The name of the web application to debug.
- **Mode.** The monitoring mode, such as Trace, Monitor, or Custom. The monitoring mode uses a collection plan to determine what is monitored. When Monitor is selected, minimal details relating to performance and exceptions are collected, and the default collection plan is used. When Trace is selected, function-level details are also collected; Trace is typically used when monitoring SharePoint applications. When Custom is selected, a customized collection plan can be used.
- **Output Path.** The location where the IntelliTrace logs should be stored.

Two additional Windows PowerShell cmdlets can be used with IntelliTrace:

- **CheckPoint-WebApplicationMonitoring.** Takes a snapshot of the IntelliTrace file, and then debugging continues
- **Get-WebApplicationMonitoringStatus.** Displays the monitoring status of all web applications currently being monitored

Enabling IntelliTrace Logging with Operations Manager

In System Center 2012 R2 Operations Manager, the IntelliTrace Profiling Management Pack is used to integrate Operations Manager with IntelliTrace and provides the ability to collect IntelliTrace logs directly from the Operations console. The IntelliTrace Profiling Management Pack deploys the IntelliTrace Collector to designated servers where debugging is required. The IntelliTrace logs are then collected and uploaded to a network file share and automatically included in alert views in the Operations console.

To enable IntelliTrace logging with Operations Manager, tasks must be performed as described in the following sections.

Importing and Configuring the Alert Attachment Management Pack

The Alert Attachment Management Pack can be found in the Management Packs folder of the Operations Manager media. This Management Pack allows Operations Manager to attach files to relevant alerts such as IntelliTrace logs. These files are stored in a network file share by Management Servers. The following high-level steps must be performed when configuring the Alert Attachment Management Pack:

1. Create a network file share where the attachments will be stored.
2. Create an Active Directory user account that has full access to the network share and is a local administrator on the Management Servers that will be used to copy files to the network share.
3. Import the Alert Attachment Management Pack.
4. Create a Run As account that uses the account created in step 2.
5. Configure the Alert Attachment Management Account Run As profile to use the Run As account created in step 4.

6. Enable the Alert Attachment file share discovery rule. This Object Discovery rule is enabled by using an override. You override the object discovery by using the For All Objects Of Class Collection Server option and then selecting the Enabled parameter. You must also specify the path to the alert attachment file share in Universal Naming Convention (UNC) format.

Importing the IntelliTrace Profiling Management Pack

After you import and configure the Alert Attachment Management Pack, you must import the IntelliTrace Profiling Management Pack, which you can find in the Management Packs folder of the Operations Manager media. This Management Pack includes the IntelliTrace tasks that are used to start, stop, and collect IntelliTrace logs. After importing the Management Pack, you must restart the Operations console to make these tasks available.

For more information about configuring integration between Operations Manager and IntelliTrace visit the following website.

 **How to Configure Integration with IntelliTrace Historical Profiling in System Center 2012 R2**

<http://go.microsoft.com/fwlink/?LinkId=404087>

Guidelines for Collecting and Viewing IntelliTrace Logs

After Operations Manager is configured to collect IntelliTrace logs, you can use the Operations console to receive IntelliTrace snapshots generated directly from .NET APM events. This information can then be used by developers to troubleshoot application performance issues and application exception errors without those developers needing to log on to the application servers to collect logging information.

Collecting IntelliTrace Historical Profiling Snapshots

When an alert such as a Server Performance Exception alert generated by APM is selected in the Operations console, the Start IntelliTrace Collection task can be used to start the collection of IntelliTrace debug logs. When running the task, you can select the Target (computers) from which the logs should be collected. You can also override the collection parameters such as the Collection Plan and Collection Duration.

After IntelliTrace collection starts, you can reproduce the issue that generated the APM alert and then select the same alert in the Operations console. Then you can use the Collect IntelliTrace Snapshot task to collect the snapshot and store it on the network share specified when you configured the Alert Attachment Management Pack. After collecting the snapshot, you should run the Stop IntelliTrace Collection task to stop the collection. This is important, because if collection is enabled indefinitely, the trace logs can consume a large amount of disk space. You can also use the Open Snapshot Location task to open the file location where the .iTrace file is stored. This task is useful because you do not need to know the network share location used when the Alert Attachment Management Pack was configured.

You collect IntelliTrace snapshots by using the following tasks:

- Start IntelliTrace Collection
- Stop IntelliTrace Collection
- Collect IntelliTrace Snapshot

Collected IntelliTrace snapshots can be opened in Visual Studio and examined by using:

- Exception Data
- Web Requests
- System Information
- Threads Lists
- Modules

Collecting IntelliTrace snapshots by Using the ASP.NET Web Application Inventory view

If there are no APM-generated alerts in the Operations console, you can still collect IntelliTrace logs from a discovered .NET web application by using either the IIS 7.0 ASP.NET Web Application Inventory view or the IIS 8.0 ASP.NET Web Application Inventory view from within the .NET Monitoring folder of the Application Monitoring node, which is in the Monitoring pane of the Operations console. When selecting an IIS application in this view, you can use the Start IntelliTrace Collection, Collect IntelliTrace Snapshot, and Stop IntelliTrace Collection tasks just as you would if you selected an APM-generated alert. After you use the Collect IntelliTrace Snapshot task, you can view the snapshot collected in the New Traces section of the New Alerts view in the IntelliTrace Profiling node, which is in the Monitoring pane in the Operations console. When selecting a snapshot here, you can open the location where the snapshot is stored by using the Open Attachment Location task.

Locating IntelliTrace snapshot Files on the Application Server

When the Start IntelliTrace task is used to start collecting trace logs, the trace files are stored locally on the application server that you run the Start IntelliTrace task on. These files can be found in the Microsoft Monitoring Agent installation folder. By default, this is C:\Program Files\Microsoft Monitoring Agent\Agent\IntelliTraceCollector\traces.

Viewing IntelliTrace Snapshot Trace Files

You can open and investigate IntelliTrace snapshots by using Visual Studio 2012 Ultimate or Visual Studio 2013 Preview. To open an IntelliTrace snapshot file in Visual Studio, on the File menu, in the Open list, click File. You then select the relevant .ITrace file that you want to open. The IntelliTrace snapshot is opened, and an IntelliTrace Summary is displayed. There are four sections within the IntelliTrace Summary that you can use to debug the exception collected in the snapshot. These five sections include:

- **Exception Data.** In the Exception Data section, each exception recorded by IntelliTrace is listed. Information such as the Exception type, Newest Message, and Newest Event Time are included for each exception. When you select an exception, you can also view the Call Stack information that relates to it. You can also search the list of displayed exceptions, which is useful when you know the exception type you are interested in and when a large number of exceptions are displayed.
- **Web Requests.** In the Web Requests section, a list of all web requests made to the web application is displayed, including information such as the Target URL, Method (such as GET or POST), Time Taken in milliseconds, Status, Client IP, and Start and End Times. You can double-click a web request to view further information such as any collected Request Events
- **System Info.** The System Info section displays information about the computer from which the IntelliTrace logs were collected, including the Computer Name, Operating System, Available Physical Bytes, Processor Speed, and bios version. This information can be useful when troubleshooting a possible resource issue, because the amount of Available Physical Bytes is displayed, which you can correlate with the time that exceptions occurred.
- **Threads List.** The Thread Lists section displays the Name, ID, Start Time, and End Time of all threads that were collected during the IntelliTrace snapshot.
- **Modules.** The Modules section displays a list of all dynamic-link library (DLL) modules that were loaded during the IntelliTrace snapshot. Information such as the Module Name, Module Path, and Module ID are included for each module. This information can be used to determine which DLLs were in use during the time an exception occurred.

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
You can use IntelliTrace only with Operations Manager.	

Lesson 3

Team Foundation Server Integration

Team Foundation Server (TFS) is an application life-cycle management tool from Microsoft that provides features for collaborative software development, such as source control, reporting, data collection, and project tracking. With System Center 2012 Service Pack 1 (SP1) and System Center 2012 R2 Operations Manager, you can integrate Operations Manager with TFS, and synchronize alerts in Operations Manager with work items in TFS. You can also convert IntelliTrace logs collected by APM into work items in TFS, and assign them to engineering.

Lesson Objectives

After completing this lesson, students will be able to:

- Describe TFS.
- Integrate TFS with System Center 2012 R2 Operations Manager.

Overview of Team Foundation Server

TFS provides application life-cycle features such as source control, work item tracking, reporting, and project management. It also includes a project portal website. Built on SQL Server, Windows SharePoint Services, and Internet Information Services, TFS provides a collaboration platform that can be used to manage the software development process, including the various teams that are involved when managing an application's life cycle.

One of the key features in TFS is work item tracking, which is possible through integration with Operations Manager. Before you understand the integration features provided by Operations Manager, however, you should first understand the function of work items in TFS.

Work items in TFS provide a method of tracking work, such as the tasks performed when troubleshooting a bug in a software application. When creating a work item in TFS, a form is used to capture the relevant details about the work item. The following list provides some examples of fields a work item can contain:

- **ID.** A unique ID number that is used to reference the work item
- **Title.** The title of the work item, such as *DLL missing from Library folder*.
- **Path.** The full path to where the work item is stored in TFS.
- **State.** The state of the work item, such as Active or Closed.
- **Assigned To.** Who the work item is assigned to
- **Severity:** The severity of the work items, such as 1 or 4
- **Description.** A full description of the work item, including any reproduction steps
- **Files.** Files that should be included with the work item
- **Links.** Any links to other related work items

Work items in TFS provide a method of:

- Recording completed work
- Viewing the history of completed work
- Recording who is working on the work item
- Sorting work items based on fields such as State or Severity



- **By.** The person who created the work item

You can create different types of work items in TFS related to the nature of the work to be completed. In the preceding list, work items relate to a bug in a software application. As users address the work item, they update relevant fields, such as the Description field where a log of completed work is recorded. Because the log shows all the work completed and the individuals who did the work, you can easily view the history of a work item.

The Process of Integrating Operations Manager with Team Foundation Server

By integrating Operations Manager and TFS, you can automatically create work items in TFS based on alerts in Operations Manager. Integration is supported in TFS 2010, TFS 2012 and TFS 2013.

Configuring Integration with TFS

To configure integration between Operations Manager and TFS, the following tasks must be performed:

1. Import and configure the Alert Attachment Management Pack as described in Lesson 2.
2. Identify the Operations Manager Management Servers that will be used for synchronization. On each Management Server, you must install the TFS Object Model.
3. Create a user account that will be used to synchronize Operations Manager alerts with TFS work items.
4. Grant the account TFS contributor permissions in each TFS project with which you plan to synchronize work items.
5. If you plan to synchronize file attachments from alerts in Operations Manager, such as IntelliTrace logs, you must also grant this account read/write access to the Alert Attachment file share that was created as part of configuring the Alert Attachment Management Pack.
6. From the Management Packs folder on the Operations Manager media, import the Microsoft.SystemCenter.TFSWISynchronization.mpb Management Pack into Operations Manager.
7. Use the Add Monitoring Wizard with the TFS Work Item Synchronization Management Pack template to configure the connection to the TFS Server. During configuration, you specify the Team Project Collection URL, the Synchronization Resource Pool, and the Synchronization Account. You then select the Project and Area Path that will be synchronized in TFS.

When integrating Operations Manager with TFS, you must:

- Install the TFS Control Object on each Management Server that will be used for synchronization
- Create a user account that has TFS contributor permissions
- Import the TFS Synchronization Management Pack
- Configure the TFS Work Item Synchronization Management Pack template

After you configure the TFS Work Item Synchronization Management Pack Template, you can right-click any alert and, from the Set Resolution State list, select the Assigned to Engineering option. This starts an Operations Manager task, named Import Operational Issue Work Item Type Task, which automatically creates a work item in TFS. Alert information such as the description, product knowledge, and custom fields are also added to the work item.

Automatically Assigning Alerts to Engineering in TFS

In addition to manually assigning alerts to engineering in TFS, you can configure Operations Manager to automatically assign alerts to engineering. This is useful when alerts with a specific resolution state should always be assigned to engineering. To configure alerts to be automatically assigned to engineering, you

override the TFS Work Items Creation rule. When overriding this rule, you must override the rule for all objects of the TFS Connector class. You then override the Assign To Engineering State Codes parameter and add a semicolon-separated list of alert resolution states. By default, alert resolution state 248 is included, which relates to the Assigned To Engineering alert resolution state in Operations Manager. If you wanted all alerts to be synchronized with TFS work items, you would add **0;248** to the Assign To Engineering State Codes parameter.

Automatically Closing Alerts When TFS Work Items Are Closed

You can also configure integration so that when work items relating to Operations Manager alerts are closed in TFS, the corresponding alerts are also closed in the Operations console. To configure this, you must override the TFS Work Item Synchronization rule. When overriding the rule, you must choose to override it based on the For All Objects Of Type: TFS Collection option. You then edit the Auto Close Alerts parameter and change its value from False to True.

For more information about configuring integration between Operations Manager and Team Foundation Server visit the following website.



Integrating Operations Manager with Development Processes in System Center 2012 R2

<http://go.microsoft.com/fwlink/?LinkId=404088>

Lab: Monitoring .NET Framework Applications

Scenario

Contoso, Ltd. provides several services to its customers, including the development of .NET web applications. These applications are also hosted in Contoso's datacenters worldwide. You are asked to provide its customers with proactive monitoring for applications who have the expected service levels for both performance and availability.

To provide the monitoring functionality that is required by Contoso, you decide to configure Operations Manager APM for the .NET web applications. You also decide to configure integration between Operations Manager and TFS so that APM-related alerts can be assigned to engineers in TFS.

Objectives

After completing this lab, students will be able to:

- Configure APM to monitor a .NET application from both the server-side and the client-side.
- Configure IntelliTrace monitoring for the DinnerNow .NET web application.
- Configure integration between Operations Manager and TFS.

Lab Setup

Estimated Time: 60 minutes

Virtual Machines: 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-MS2, 10964C-LON-AP2, 10964C-LON-AP1

User Name: Contoso\Administrator

Password: Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps.

1. On LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, in Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Domain: **Contoso**
5. Repeat steps 2–4 for the following virtual machines:
 - 10964C-LON-SQ1 (On LON-HOST1)
 - 10964C-LON-MS1 (On LON-HOST2)
 - 10964C-LON-MS2 (On LON-HOST1)
 - 10964C-LON-AP2 (On LON-HOST2)
 - 10964C-LON-AP1 (On LON-HOST1)



Note: Before you start this lab, make sure that all Windows Services that are set to start automatically are running. The exception is the Microsoft .NET Framework NGEN v4.0.30319_X86 and .NET Framework NGEN v4.0.30319_X64 services, because these services stop automatically when they are not being used.

Exercise 1: Monitoring .NET Applications

Scenario

To monitor .NET web application in Operations Manager, you must configure APM. In this exercise, you use the .NET Application Performance Monitoring template to configure monitoring for the DinnerNow .NET application.

The main tasks for this exercise are as follows:

1. Import the APM Management Pack for IIS
2. Configure application performance monitoring
3. Restart IIS
4. Browse the DinnerNow website and view application performance alerts
5. Simulate a database failure in DinnerNow and view application performance alerts
6. Use Application Advisor to view application performance monitoring reports

► Task 1: Import the APM Management Pack for IIS

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Open the Operations console and import the **Microsoft.SystemCenterAPM.Web.IIS7.mp** Management Pack from **\LON-DC1\Media\SCOM2012R2\ManagementPacks**

► Task 2: Configure application performance monitoring

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Authoring
View	Management Packs Templates

2. Use the Add Monitoring Wizard to configure the **.NET Application Performance Monitoring** template with the following settings (all other settings should remain as the default settings):
 - Name: **DinnerNow**
 - Management Pack: Create a new Management Pack named **DinnerNow**
 - What to Monitor: **DinnerNow**
 - Monitoring Scope: **Production**
 - Server-Side Configuration\Performance event threshold: **50**
 - Enable additional configuration options for server-side and client-side monitoring
 - Server-side Customization\Customize: **Enable Application Failure Alerts** and **All Exceptions**
 - % Exception Events/sec exceeds threshold: **1**
 - % Performance Events/sec exceeds threshold: **1**
 - Average Request Time exceeds threshold: **10**
 - Client-side Configuration: **Turn on exception event alerts**
 - Page load threshold (ms): **5**
 - Ajax and WCF threshold (ms): **5**
 - Configure client IP address filter: **Remove both filters**
 - Advanced Settings\ Sensitivity threshold (ms): **5**
 - % Exception Events/sec exceeds threshold: **1**
 - % Performance Events/sec exceeds threshold: **1**
 - Average Request Time exceeds threshold: **10**
 - Enable Client-Side Monitoring: **Enabled**

► Task 3: Restart IIS

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring\Operations Manager
View	APM Agent Details\IIS Restart / Recycle Required

2. Select **LON-AP2**, and then use the **Restart Internet Information Services** task to restart IIS on LON-AP2.



Note: It can take about five minutes for LON-AP2 to appear.

► Task 4: Browse the DinnerNow website and view application performance alerts

1. To perform this task, use the computer and tool information shown in the following table.

Location	Value
Computer	LON-AP2
Tool	Internet Explorer
URL	http://LON-AP2/DinnerNow
Your Zip	98101

2. Browse to the **DinnerNow** website, enter the zip code, and using the **Northwind Bar & Grill** details, add **Mango Smoothie** to the shopping cart.
3. Try to add **Sweet Pudin** to the shopping cart
4. Open the Operations console on LON-MS1, and from the **Monitoring** pane, open the **Application Monitoring\Net Monitoring\Active Alerts** view
5. Open the properties of one of the **Server Performance Exception** alerts.
6. On the **General** tab, click the hyperlink to open the Application Diagnostics console.
7. Notice the custom handler that has caused the alert to occur based on the threshold breach
8. In the **Performance Counters** tab, review, the **Diagram** view, and **Table** view

► **Task 5: Simulate a database failure in DinnerNow and view application performance alerts**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-AP2
Tool	DinnerNow SQL DB Detacher
Location	Desktop
Status	Stop

2. Use the **DinnerNow SQL DB Detacher** utility to detach the DinnerNow SQL database.
3. On LON-MS1, start Windows Internet Explorer, and then browse to **http://LON-AP2/DinnerNow**.
4. Notice the drop-down menus are empty.
5. From the **Monitoring** pane, open the Operations console, and then open the **Application Monitoring\Net Monitoring\Active Alerts** view.
6. Notice the **Server Application Exception** alerts.
7. View the **Alert Details** pane, and then open an alert that includes **Cannot open database** in the description.
8. From the **General** tab, click the hyperlink to open the Application Diagnostics console.
9. View the details on the **Event properties** tab to determine the cause of the failure.

10. View the **Related events** tab and notice the events that are related to this event, such as **500 Internal Server Error**.
11. From the **Performance counters**, view the performance counter data that is collected.
12. On LON-AP2, reattach the SQL database for DinnerNow by using the **DinnerNow SQL DB Detacher**.

► **Task 6: Use Application Advisor to view application performance monitoring reports**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Internet Explorer
URL	http://LON-MS1/AppAdvisor
Report	Application Failure Analysis

2. Run the **Application Failure Analysis Report**.

- Source: **DinnerNow – Production**

Results: After this exercise, you should have configured Application Performance Monitoring for the DinnerNow .NET application, including monitoring the application from both the server-side and the client-side. You should have also used the Application Diagnostics and Application Advisor consoles to view exception and performance data for the application.

Exercise 2: Configuring IntelliTrace

Scenario

To assist with troubleshooting exception errors that are occurring, Contoso's development team has requested IntelliTrace logging be enabled on one of the application servers that hosts a .NET web application. To facilitate this, you must install and configure the Alert Attachment Management Pack and then install the IntelliTrace Profiling Management Pack. You then use the Operations console to enable IntelliTrace logging on the application server and collect IntelliTrace logs.

The main tasks for this exercise are as follows:

1. Create a network file share to store IntelliTrace logs
2. Create a Run As account
3. Import the Alert Attachment Management Pack
4. Configure the Alert Attachment Management Pack
5. Import the IntelliTrace Profiling Management Pack
6. Collect IntelliTrace profiling snapshots
7. View IntelliTrace snapshots in Visual Studio

► Task 1: Create a network file share to store IntelliTrace logs

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Windows Explorer
Folder	C
Folder to create	Alert_Attachments

2. Create the **Alert_Attachments** folder on Drive C of LON-MS1, and then share it by using read/write permissions for everyone.

► Task 2: Create a Run As account

1. To perform this task, use the computer and tool information shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Run As Configuration\Accounts

2. Create a Run As account with the following settings (leave all other settings as the default settings):
 - Display name: **Alert Attachment Account**

- User name: **Contoso\Administrator**
 - Password: **Pa\$\$w0rd**
 - Distribution Security: **More secure**
3. Edit the distribution settings of the Run As account, and then add the **LON-MS1.CONTOSO.COM** computer.

► Task 3: Import the Alert Attachment Management Pack

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Import the **Microsoft.SystemCenter.AlertAttachment.mpb** Management Pack from \\LON-DC1\Media\SCOM2012R2\Management Packs.

► Task 4: Configure the Alert Attachment Management Pack

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Run As Configuration\Profiles

2. Edit the **Alert Attachment Management Account** with the following setting (all other settings should remain the default settings):
 - Run As Account: **Alert Attachment Account**
 - From the **Authoring** pane open the **Object Discoveries** view from the **Management Pack Objects** folder.
 - Use the **Change Scope** button to change the scope and find the **Alert Attachment File share** object discovery.
3. Override the **Alert Attachment File Share discovery** for **all objects of class Collection Server**, and then override the following parameters:
 - Enabled: **True**
 - Path to the alert attachment file share: **\LON-MS1\Alert_Attachments**

4. Store the override a in a new Management Pack named **Alert Attachment Management Pack Overrides**.

► **Task 5: Import the IntelliTrace Profiling Management Pack**

1. To perform this task, use the computer and tool information shown in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Import the **Microsoft.SystemCenter.IntelliTraceProfiling.mpb** Management Pack from \\LON-DC1\Media\SCOM2012R2\Management Packs.
3. Restart the Operations console.
4. Wait until LON-MS1 appears in the **IntelliTrace Profiling\State** view in the **Monitoring** pane and its state is displayed as **Healthy**.

► **Task 6: Collect IntelliTrace profiling snapshots**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Monitoring
View	Application Monitoring\.NET Monitoring\Active Alerts

2. From the **Active Alerts** view, select a **Server Performance Exception** alert, and then use the **Start IntelliTrace Collection** task to start the IntelliTrace collection.
3. Browse to the **DinnerNow** website on LON-AP2, and from the **Northwind Bar and Grill** site, add **Item # 1** and **Item # 0** to the shopping cart. The script error is expected when selecting Item # 0.
4. Use the **Collect IntelliTrace Snapshot** task to collect the IntelliTrace snapshot.
5. Use the **Stop IntelliTrace Collection** task to stop IntelliTrace collection.
6. Use the **Open Attachment Location** task to confirm the trace file has been collected.

► **Task 7: View IntelliTrace snapshots in Visual Studio**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-AP1
Tool	Visual Studio 2013
File	iTrace file
Locations	\LON-MS1\Alert_Attachments

2. Open the **iTrace** file from the **Alert_Attachments** share in Visual Studio, and then review the IntelliTrace data that has been collected in the following sections:

- **Exception data**
- **Web Requests**
- **System Info**
- **Threads List**
- **Modules**

Results: After this exercise, you should have installed and configured the Alert Attachment Management Pack and then installed the IntelliTrace Profiling Management Pack. You should also have used the Operations console to start IntelliTrace logging and collected an IntelliTrace log from the .NET web application server.

Exercise 3: Configuring TFS Integration

Scenario

For the development team to view APM-generated alerts for the .NET web application server, you must configure Operations Manager integration with TFS. This will allow alerts in Operations Manager to be synchronized with work items in TFS.

The main tasks for this exercise are as follows:

1. Import the TFS Work Item Synchronization Management Pack
2. Configure the TFS Work Item Synchronization Management Pack template
3. Confirm TFS integration is working as expected

► Task 1: Import the TFS Work Item Synchronization Management Pack

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Administration
View	Management Packs

2. Import the **Microsoft.SystemCenter.TFSWISynchronization.mpb** Management Pack from \\LON-DC1\Media\SCOM2012R2\Management Packs.

► Task 2: Configure the TFS Work Item Synchronization Management Pack template

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	LON-MS1
Tool	Operations Console
Pane	Authoring
Management Pack Template	TFS Work Item Synchronization

2. Use the Add Monitoring Wizard to configure the **TFS Work Item Synchronization** Management Pack Template with the following settings (leave all other settings as default settings):

- Name: **Contoso TFS Environment**
- Management Pack: Create a new Management Pack named **Contoso TFS Management Pack**.
- Team Project Collection URL: **http://lon-ap1:8080/tfs/Contoso/**
- Synchronization Resource Pool: Create a new **Resource Pool** named **LON-MS2** and add **LON-MS2 to the Resource Pool**
- Synchronization Account: **Alert Attachment Account**

- Project: **Contoso Team Project**
 - Area Path: **Contoso Team Project**
 - Password: **Pa\$\$w0rd**
3. Save the configuration.
 4. Logon to LON-AP1 and create a folder in **C** name **TFS**.
 5. Browse to \\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64.
 6. Copy the **OperationalIssue_11.xml** file to the **C:\TFS** folder on LON-AP1.
 7. Open a command prompt and navigate to the **C:\TFS** folder.
 8. Type the following command and then press enter:
- ```
C:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\witadmin.exe"
importwitd /collection:http://lon-ap1:8080/tfs /p:"Contoso Team Project"
/f:OperationalIssue_11.xml
```
9. Wait until the message stating **The work item type import has completed** appears and then close the command prompt window.

#### ► Task 3: Confirm TFS integration is working as expected

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                         |
|----------|---------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                |
| Tool     | <b>Operations Console</b>                                     |
| Pane     | <b>Monitoring</b>                                             |
| View     | <b>Application Monitoring\\$.NET Monitoring\Active Alerts</b> |

2. Set the **Resolution State** for a **Server Performance Exception** alert to **Assigned to Engineering**.
3. From the Tasks Status view, wait until the **TFS Create Work Item Task** is displayed.
4. Open **Visual Studio 2013** on LON-AP1.
5. Use the **New Query** option to open the **Work Items** view.
6. Review the new work item that has been created for the **Server Performance Exception** alert.

**Results:** After this exercise, you should have installed and configured the TFS Work Item Synchronization Management Pack. You should have also configured the TFS Work Item Synchronization Management Pack Template. Finally you should have confirmed TFS integration is working by assigning an alert to engineering in the Operations console, and then confirming a work item was created in TFS.

**Question:** You are configuring the .NET Application Performance Monitoring Management Pack template for a .NET web application. You have to make sure that the application is monitored from every network location. What must you do?

**Question:** When configuring integration between Operations Manager and TFS, what must be installed on each Management Server that will be used for synchronization?



# Module Review and Takeaways



## Best Practice: Client-side Monitoring Data Collection in APM

It is recommended that the Global Variables and Exception Stack data items be used only when the application is configured for HTTPS, because the Global Variables and Exception Stack data items send application data to the monitored server, and this might be considered sensitive data.

## Common Issues and Troubleshooting Tips

| Common Issue                                                                                                                                                                                   | Troubleshooting Tip |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| When using the Add Monitoring Wizard to configure the TFS Work Item Synchronization Management Pack Template, you might find that no TFS Projects are discovered on the Project Settings page. |                     |

## Review Question(s)

**Question:** You have installed the Alert Attachment Management Pack to enable centralized management of IntelliTrace logs collected by Operations Manager. However, after running IntelliTrace, the logs are not being copied to the network share. What could be the cause of this?

## Real-world Issues and Scenarios

When you use APM to monitor .NET Framework applications, sometimes you might have to make sure that sensitive data, such as credit card information or passwords, are not collected. You can configure Operations Manager to either mask sensitive data with an asterisk, or you can configure APM to avoid collecting sensitive data completely.

## Tools

### TFS Object Model

The TFS Object Model must be installed on each Management Server that you plan to use in TFS synchronizations. You can download the Team Foundation Server 2010 SP1 Object Model Installer from here:

<http://go.microsoft.com/fwlink/?LinkId=391272>

# Module 6

## End to End Service Monitoring

### Contents:

|                                                       |             |
|-------------------------------------------------------|-------------|
| Module Overview                                       | 6-1         |
| <b>Lesson 1: Management Pack Templates</b>            | <b>6-2</b>  |
| <b>Lesson 2: Distributed Application Models</b>       | <b>6-18</b> |
| <b>Lesson 3: Global Service Monitor</b>               | <b>6-27</b> |
| <b>Lesson 4: Real-Time Visio Dashboards</b>           | <b>6-33</b> |
| <b>Lab: Configuring End-to-End Service Monitoring</b> | <b>6-38</b> |
| Module Review and Takeaways                           | 6-52        |

## Module Overview

You need to monitor key line-of-business applications from both the datacenter and end-user perspectives. In this module, you will learn how you can create synthetic transactions to measure end-user performance.

You will also learn how to combine component monitoring with synthetic transactions in distributed application models that describe the relationship between the various components of an application. This provides a single view for identifying root cause and impact of any potential service outage.

Finally, you will learn how to build rich Microsoft Visio dashboards to show real-time health to external users.

### Objectives

After completing this module, students will be able to:

- Configure Management Pack templates.
- Create distributed application models.
- Use Global Service Monitor.
- Create real-time Visio dashboards.

## Lesson 1

# Management Pack Templates

Management Pack templates in Microsoft System Center 2012 R2 Operations Manager provide a quick and simple method of creating customized monitoring in Operations Manager. By using the Add Monitoring Wizard, you can select a specific template to create multiple rules and monitors that are targeted at specific objects or components.

For example, you might want to monitor a Windows service, which is not covered by an out-of-the-box Management Pack. By running through a few simple pages of a wizard, you can create monitors that provide information about the health and performance of the service, rules that collect performance and event data along, and a discovery that identifies the target service.

It is important to understand what Management Pack templates are available in Operations Manager so that you can use them in your environment to further enhance Operations Manager monitoring capabilities.

Note that the .NET Application Performance Monitoring Management Pack template, which was covered in Module 5, is not discussed in this module.

### Lesson Objectives

After completing this lesson, students will be able to:

- Configure the OLE DB Data Source Management Pack template.
- Configure the Process Monitoring Management Pack template.
- Configure the TCP Port Management Pack template.
- Configure the UNIX/Linux Log File Monitoring Management Pack template.
- Configure the UNIX/Linux Process Monitoring Management Pack template.
- Configure the Web Application Availability Monitoring Management Pack template.
- Configure the Web Application Transaction Monitoring Management Pack template.
- Configure the Windows Service Management Pack Template.

### Guidelines for Configuring the OLE DB Data Source Management Pack Template

Many web applications rely on a back-end database to collect and store data used by the application. If the database is unavailable or performance is decreased, end users will have issues performing their day-to-day tasks. To test the performance and availability of the database, the OLE DB Data Source Management Pack template can be configured to monitor connectivity and run queries. You can monitor connectivity and run queries from multiple locations that simulate the application's access to the database. You configure the template by using the Add Monitoring Wizard. To access a wizard, in the Operations console, in the Authoring pane, in the Tasks pane, select any Management Pack template.

**The OLE DB Data Source Management Pack template configures:**

- Connection string
- Query performance
- Watcher nodes



The following table describes each page of the Add Monitoring Wizard that is used to configure the OLE DB Data Source Management Pack template, including the available settings.

| Add Monitoring Wizard page when configuring the OLE DB Data Source Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                          | Add a name for the monitor, and either select or create a new Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Connection String                                                                           | Specify the connection details that are used to connect to the OLE DB Data Source. You can manually type the details, or use the Build button to add the provider, such as the Microsoft OLE DB Provider for SQL Server; the computer or device name; and the database name. Using the Build button to create the connection string, rather than manually typing the information, can prevent syntax errors. You can add a query to execute, such as <code>select * from dbo.alerts</code> , that will be used to test both access to the database and performance of the results returned by the query. Additionally, you can test the connection and query to confirm that the connection string and query are configured correctly. |
| Query Performance                                                                           | Set timing thresholds, such as Connection Time In Milliseconds, Query Time In Milliseconds, and Fetch Time In Milliseconds. Then, specify an error threshold and warning threshold for each performance setting. These thresholds generate alerts when they are breached.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Watcher Nodes                                                                               | Select the agent-managed computers that will be used to run the tests. These computers should be a representation of your end-user base, and an Operations Manager agent should be installed on a client or server in each location and then selected as a watcher node. You also specify how frequently the test should be run. The default is every two minutes.                                                                                                                                                                                                                                                                                                                                                                     |
| Summary                                                                                     | A summary of the settings that you configured is displayed so that you can confirm the settings and either create the monitor or go back through the wizard to make any changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

After you complete the Add Monitoring Wizard, the OLE DB Data Source monitor starts to monitor the database immediately from the locations that you specified on the Watcher Nodes page of the wizard.

### **Viewing Performance and Availability of an OLE DB Data Source**

When the OLE DB Data Source monitor is running, alerts that are generated can be viewed in the Active Alerts view of the Monitoring pane in the Operations console. For example, if the Error Threshold that is specified for the Connection Time In Milliseconds Setting is breached, a Connection Time alert is generated. The alert details show the actual connection time and the configured threshold times. You can use this information when you perform a baseline, which can help you determine optimal threshold values during regular operation times. The Full Path indicated the alert detail also shows which agent-managed computer on which the test has failed.

You can also view the health state of the OLE DB Data Source monitor, by selecting the OLE DB Data Source State view from in the Synthetic Transactions folder of the Monitoring pane. This view provides an overall view of the monitor's health state. The Yellow state indicates a Warning threshold is breached, the Red health state indicates an Error threshold is breached, and the Green health state indicates that the monitor is healthy. A state for each watcher node is included here, so you can view the health state from each location being monitored.

In the Synthetic Transaction folder, you can also view the performance counters that are collected for the monitor. Right-click the monitor and then click Open and then click Performance View. Select Connection Time, Fetch Time, and Execution Time counters to build a graph for viewing performance for each watcher node over a selected time period. You can use the counters to troubleshoot a Warning or Critical health state, both of which provide immediate information about what is causing a threshold breach.

More information about the OLE DB Data Source template can be found on the following link:

 **OLE DB Data Source Template**

<http://go.microsoft.com/fwlink/?LinkId=321885>

## Guidelines for Configuring the Process Monitoring Management Pack Template

You use the Process Monitoring Management Pack template to monitor the behavior of processes that should be running on an agent-managed computer, or to monitor the behavior of processes that should not be running on an agent-managed computer. For example, suppose you have a critical line-of-business application that, to function, relies on a particular process running at all times. Using the Process Monitoring Management Pack template, you can quickly create a monitor that generates an alert when this process is not running. In another scenario, there might be a particular process that should not be running on agent-managed computers, such as a process that is known to have a memory leak. In this case, you can use the Process Monitoring Management Pack template to create a monitor that generates an alert if the process is found to be running. After the monitor is configured, Operations Manager creates a new process class and the appropriate monitors for the class. This class is then discovered on the target computers, and the instances can be added to distributed application diagrams or state views.

**The Process Monitoring Management Pack template can be used to:**

- Determine how long a process has been running
- Detect if a process is running
- Detect if a process is not running
- Record the memory and CPU usage of a running process

To configure the Process Monitoring Management Pack template, you must use the Add Monitoring Wizard in the Operations console. The following table describes each page of the Add Monitoring Wizard that is used to configure the Process Monitoring Management template, including the available settings.

| Add Monitoring Wizard page used to configure the Process Monitoring Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                           | Specify a name for the monitor and optionally include a description. The description can be used to provide an overview of which process is being monitored and the reason for monitoring it. You also select or create a Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Process to Monitor                                                                           | Select the Monitoring scenario. Choose the option to monitor whether and how a process is running, or choose to monitor only whether the process is running. In either case, you must then provide the full name of the process to be monitored. You can browse to select the process executable or manually enter the process name. You must also provide a targeted group, which contains the computers on which the process should be monitored.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Running Processes                                                                            | If the Monitor Whether And How A Process Is Running option is selected on the Process To Monitor page, on the Running Processes page, you can select when an alert should be generated for the running process. For example, you can generate an alert when the minimum number of processes reaches a specific value, or when the maximum number of processes reaches a specific value over a configured duration. Alternatively, you can generate an alert if the process runs for longer than a specified duration. If the Monitor Only Whether The Process Is Running Option is selected on the Process To Monitor page, then options on the Running Processes page are not available.                                                                                                                                                                                              |
| Performance Data                                                                             | If the Monitor Whether And How A Process Is Running option is selected on the Process To Monitor page, you can configure, on the Performance Data page, an alert that will be generated based on memory or CPU usage. This can be useful when monitoring a process that is known to consume large amount of memory or CPU resources. An alert can be triggered, and optionally a recovery task created, that restarts a service that uses the monitored process. You can optionally configure the number of samples that should be taken and a sample interval. You might do this, for example, when you want to generate an alert only if the process is consuming 90 percent of CPU resources for more than 5 minutes. If the Monitor Only Whether The Process Is Running option is selected on the Process To Monitor page, options on the Performance Data page are not available. |
| Summary                                                                                      | A summary of the settings you configured. This lets you confirm the settings and either create the monitor or go back through the wizard to make changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

After the monitor is created, the defined process is monitored on the computers selected in the targeted group, which you specified on the Process To Monitor page of the wizard.

### Viewing the Health State of Process Monitors

You can view the health state of monitored processes in the Process State view of the Windows Service and Process Monitoring folder, in the Monitoring pane of the Operations console. For each instance of a process being monitored, its health state, display name, process name, and path are displayed. You can also open other views from here, such as the alert view or performance view, which is useful when you need to determine how much memory or CPU resources a process has consumed over a given time period.

### Viewing Alerts generated by a Process Monitor

When a process monitor generates an alert, the alert can be viewed in the Active Alerts view in the Monitoring pane of the Operations console. Included in the alert are a description, the name of the process, and how long the process has been running. Other details such as the Source and Full Path Name are displayed in the Alert Details section. You can use this information to determine which computer the alert was generated for.

## Guidelines for Configuring the TCP Port Management Pack Template

Use the TCP Port Management Pack template to check the availability of a TCP/IP port. You can use this template to monitor website connectivity, because it can be configured to check for the availability of port 80. Port 80 is the default port used by most common websites. If the website is secured by using the Secure Sockets Layer (SSL) protocol, port 443 can be monitored for connectivity. Although typically used for website connectivity monitoring, the template can be used for many other applications that are accessed over a TCP/IP port, including port 21 for an FTP server or port 25 for an SMTP server. The template can also be used to monitor connectivity to network devices such as a router or a bridge.

**The TCP Port Management Pack template configures the following:**

- Target and port
- Watcher nodes



To configure the TCP Port Management Pack template, you must use the Add Monitoring Wizard in the Operations console. The following table provides describes each page of the Add Monitoring Wizard used to configure the TCP Port Management template, including the available settings.

| Add Monitoring Wizard page used to configure the TCP Port Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                 | Add a name for the monitor, and either select or create a new Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                   |
| Target and Port                                                                    | Add the computer or device name in the form of a NetBIOS name, FQDN name, or IP address. Add the port that should be tested for connectivity. A Test button is also provided for testing connectivity from the Management Server. You must be aware that the Management Server might be on a different network from the watcher nodes and the TCP port that is being monitored. Therefore, you should consider this when you test for connectivity. |
| Watcher Nodes                                                                      | Select the agent-managed computers that will be used to run the                                                                                                                                                                                                                                                                                                                                                                                     |

| Add Monitoring Wizard page used to configure the TCP Port Management Pack template | Description                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                    | tests. The computers that you select on this page should be a representation of your end-user base. An Operations Manager agent should be installed on a client or server in each location and then selected on this page as a watcher node. You also specify how frequently the test should be run. By default, this is every two minutes. |
| Summary                                                                            | A summary of the settings you configured is displayed. You confirm the settings, and then either create the monitor or go back through the wizard and make changes.                                                                                                                                                                         |

After completing the Add Monitoring Wizard, the TCP port monitor starts to monitor the TCP port immediately. The monitoring is from the locations that are specified in the Watcher Nodes page of the wizard.

### Viewing Connectivity to a TCP Port

When the TCP port monitor is running, any connectivity failures generate an alert in the Active Alerts view in the Monitoring pane. For example, if a watcher node tries to connect to a port that it is not permitted to connect to, a Connection Refused alert is generated. The alert details provide the node that failed the test, the computer or device name, and the port that the node tried to connect to.

The health state of TCP port monitors can also be viewed in the TCP Port Checks State view from the Synthetic Transactions folder in the Monitoring pane. You can also open the Performance View from this folder. In this view, you can select the Connection Time counter to display a graph that shows the connection time, in milliseconds, over a specified time period. You can use graph to troubleshoot connectivity issues and identify peak times of the day when connection to the port is taking longer than expected.

More information about how to create a TCP port monitor can be found on the following link.



#### How to Create a TCP Port Monitor

<http://go.microsoft.com/fwlink/?LinkId=321886>

## Guidelines for Configuring the UNIX/Linux Log File Monitoring Management Pack Template

Use the UNIX/Linux Log File Monitoring Management Pack template to detect specific strings of text written to a UNIX or Linux log file, for example, a syslog file. This template is useful when you need to detect text that represents a failure in an application, such as an error code.

To configure the Unix/Linux Log File Monitoring Management Pack Template, you must use the Add Monitoring Wizard in the Operations console. The following table provides describes each page of the Add Monitoring Wizard that is used to configure the UNIX/Linux Log File Monitoring Management Pack template, including the available settings.

#### The UNIX/Linux Log File Monitoring Management Pack template provides:

- Monitoring of log files for text strings on computers running UNIX and Linux
- Alerts when specified text expressions are detected

| Add Monitoring Wizard page used to configure the UNIX/Linux Log File Monitoring Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                                       | Specify a name for the monitor and optionally include a description. You also select or create a Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Log File Details                                                                                         | Specify the monitoring target first, which is a computer or computer group. For the computer, you select from a list of agent-managed computers running UNIX or Linux. For the computer group, you select the group that contains the computers running UNIX and/or Linux against which the monitor will be run. You then specify the log file monitoring settings, including the log file path, the expression of text that should be searched, the Run As profile that should be used to access, the log file, and the alert severity, such as Error, Warning, or Information, which is generated when the specified text is detected. A Test button is also provided on this page, which is useful when you need to test complex expressions that you want to detect in a log file. When testing, you add the regular expression to detect and then include a sample entry. You then click the Test button and either a Match Found or Match Not Found result is displayed. |
| Summary                                                                                                  | A summary of the configured settings is displayed. This lets you confirm the settings and either create the monitor or go back through the wizard to make changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

For each expression of text that is detected in the log file, an alert is generated in the Active Alerts view in the Monitoring pane of the Operations console. In Alert Details, you can view which expression was detected, including the log file it was detected in and the computer running UNIX or Linux computer on which the log file resides.

## Guidelines for Configuring the UNIX/Linux Process Monitoring Management Pack Template

The UNIX/Linux Process Monitoring Management Pack template is used to monitor a process running on a UNIX-based or Linux-based computer. This template can be useful when you need to ensure a specific application is running, such as a firewall application. If the process that the application uses is found not to be running, an alert can be generated.

To configure the UNIX/Linux Process Monitoring Management Pack template, you must use the Add Monitoring Wizard in the Operations console. The following table describes each page of the Add Monitoring Wizard that is used to configure the UNIX/Linux Process Monitoring Management Pack Template, including the available settings.

### The UNIX/Linux Process Monitoring Management Pack template provides:

- Monitoring the number of processes running on a UNIX-based or Linux-based computer
- Filtering of the process instance names to target a process appropriately
- Alerting when the number of process instances falls below or is greater than a specified value



| Add Monitoring Wizard page used to configure the UNIX/Linux Process Monitoring Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                                      | Specify a name for the monitor and optionally include a description. You also select or create a Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Details                                                                                                 | Either enter a process name to monitor and then specify the computer group to target, or browse to select a computer and process to monitor. With the latter option, the process is monitored only on the selected computer. You also specify the alert severity, such as Error, Warning, or Information, of the alert generated in the Operations console. Optionally, you can also specify a regular expression to filter process arguments. This is useful when you need to filter processes that might have a similar name, because it allows you to target monitoring to the specific instance of a process. If you use the Select A Process option to connect to a computer and select a process, a list of processes with the process name is displayed. You can then use the Regular Expression To Filter The Process Arguments option to view how the filter will be applied and view which processes will be monitored. |
| Settings                                                                                                | Configure the process monitoring settings, including whether an alert should be generated when the number of process instances falls below a specified value. You can also specify that an alert should be generated when the number of process instances is greater than a specified number. This can be useful when you know that when a certain number of running process instances constitutes an application failure or resource issue for example.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Summary                                                                                                 | A summary of the configured settings is displayed. You confirm the settings, and then either create the monitor or go back through the wizard to make changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

After creating a UNIX/Linux process monitor, any alerts that are generated will be shown in the Active Alerts view in the Monitoring pane on the Operations console. Additionally, you can open the Health Explorer for a monitored object in the UNIX/Linux view in the Monitoring pane, and then view the health state of each monitor created.

## Guidelines for Configuring the Web Application Availability Monitoring Management Pack Template

The Web Application Availability Monitoring Management Pack template can be used to monitor the availability of one or more web application URLs. You can run these tests either from an internal location or by using an agent-managed computer (watcher node). Or, you can run these tests from an external location by using the Global Service Monitor.

 **Note:** The Global Service Monitor is discussed in detail later in this course.

**The Web Application Availability Monitoring Management Pack template configures the following:**

- What to monitor
- Where to monitor from
- View and Validate tests
- Change configuration



The Web Application Availability Monitoring template is configured by using the Add Monitoring Wizard. The following table describes each page of the Add Monitoring Wizard that is used to configure the Web Application Availability Monitoring Management Pack template, including the available settings.

| Add Monitoring Wizard page used to configure the Web Application Availability Monitoring Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General                                                                                                           | Add a name for the monitor and select or create a new Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| What to Monitor                                                                                                   | Add the URLs of the web application to be monitored, including the name for each URL. You can achieve this in several ways: enter the URLs manually; import a CSV file that contains the URLs in the format of <i>Name, URL</i> ; or paste a copied URL from a website. Both HTTP and HTTPS web applications can be tested.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Where to Monitor From                                                                                             | Search and add either the watcher nodes (agent-managed computers) or a resource pool from which the web application will be tested. Typically, an agent-managed computer exists in the location for each end user. You add the agent-managed computers on this page as watcher nodes that will be used to test the web application simulating an end user accessing the application from the locations specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| View and Validate Tests                                                                                           | A Test list is displayed that shows each URL to be tested and each location from where the URL will be tested. You can use this list to select a specific URL and location, and then click the Run Test button to test availability. The test is run from the selected location, and a detailed report is displayed that includes the Domain Name System (DNS) resolution time, HTTP status code, total response time, and response body time. Use this information to fine-tune the tests and change the configuration for all tests that are based on the test just performed. The HTTP request, HTTP response, and raw data information that is returned from the test is also displayed when you click the Run Test button. Because the HTTP Response data include details about errors generated when accessing the URL, you can use it to troubleshoot failed tests. |

| Add Monitoring Wizard page used to configure the Web Application Availability Monitoring Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View and Validate Tests\Change Configuration                                                                      | Click the Change Configuration button to fine-tune the configuration that will be used for all tests, including the test frequency and performance data collection interval. You can also configure error and warning alerts to be generated based on criteria such as transaction response time, HTTP status code, and content. You can also configure the number of consecutive times criteria should fail before an alert is generated. This helps during heavy load scenarios where you expect tests to fail a certain number of times, for example, during a backup of an application. Several Performance Collection options can be selected, such as Response Time, TCP Connect Time, and Content Time. These help monitor and compare the end user's web application experience at each tested location. You can also include the proxy server information that the tests should use when they are accessing the web application. |
| Summary                                                                                                           | A summary of the configured settings is displayed. You confirm the settings, and either create the monitor or go back through the wizard to make changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

After completing the Add Monitoring Wizard, the Web Application Availability Monitoring monitor starts to monitor the URLs immediately from the specified locations.

Be careful when you select performance data to collect as part of this monitor. Collecting lots of data can affect the OperationsManager and OperationsManagerDW sizing requirements.

### Viewing Web Application Availability

You can view Web Application Availability by using the views that are located in the Web Application Availability Monitoring folder. This folder is located in the Application Monitoring folder, in the Monitoring pane of the Operations console.

The Active Alerts view displays alerts that are generated for each test in each location. For example, if a test could not connect to a URL from a specific location, a Web Application Unavailable alert would be generated. The Alert Details view shows the source of the alert, which in this example is the location. Opening the alert and clicking the Alert Context tab displays a detailed report that includes the results from the test. This can help you troubleshoot failed tests. Included are details such as the transaction error code, transaction response time, and several base page results, such as download time and DNS resolution time. Use all this information to quickly determine the cause of the alert.

The Test State view displays the health state for each test and the location from which the test is running. You can use this at-a-glance view to immediately determine whether a test is generating a warning or critical health state from any location. When you select a state, the Detail view displays the details of the test, including the full path name, parameters, and test configuration—helpful when you want only to view test details as opposed to edit the test. By right-clicking a state, you can open the Performance view, which displays each performance counter being collected for the test. Use this view to troubleshoot test failures, because you can quickly view (by using a graph) response time details, such as DNS resolution time, content time, and download time. You can also configure the time range you want the data displayed. You can correlate this performance data with other events that are occurring in the environment as described in the scenario below.

As an example, consider the following scenario. End users in New York complain that a web application always performs poorly during the hours of 4:00 P.M. and 5:00 P.M. By using the Test State view, you

notice the test state for the New York location is unhealthy and shows a warning state. You open the Performance view for the location and select the Response Time Performance counter. You set the Time Range to between 9:00 P.M. and 10:00 P.M., because the application is hosted in the United Kingdom where the time difference is five hours ahead of New York. The graph displays a sharp increase in Response Time during the time range. This confirms that the test from the New York location is performing poorly during this time. You realize a backup of the application is being performed. Therefore, this would be the cause of the poor performance that is experienced by end users in the New York office.

The Web Application Status view displays the overall health state of the web applications that are being monitored and quickly shows you how the application is performing. For each web application, a health status of Green (Healthy), Yellow (Warning), or Red (Critical) is displayed.

To display a detailed dashboard, select an application in the Web Application Status view and then, in the Tasks pane, click the Detailed Dashboard – List task. This dashboard shows performance counter data for the application, including Total Transaction Time, DNS Resolution Time, and Content Size. Select one or more tests from the Test Status section to display dashboard updates for the related performance counter data for the selected test. You can use this to compare data from multiple locations. For example, you can select a test from New York and London. Then, you can compare the DNS Resolution Time and Total Transaction Time to compare the end users' experience of the application from both locations at the same time.

The Summary Dashboard shows how an application is performing globally and lets you immediately view the location where end users are experiencing issues. Use the Summary Dashboard – Map task to display a map of the world; each location where a test is being performed is highlighted. The Map task also includes the health state of the test. Select a location to display the Test Status pane with the Transaction Response Time(s), Sample Time, and Location of the tests being performed at the selected location displayed.

The Health Explorer can also be used to monitor and troubleshoot the health and performance of the web application. Right-click a test, point to Open, and then click the Health Explorer to open the Health Explorer. By default, the Scope is set to unhealthy child monitors. However, the Scope can be removed so that all monitors are displayed and their health state is included. By selecting a monitor such as Web Application Monitor, the Details pane displays Knowledge that relates to the monitor. This can include possible causes for the monitor being in an unhealthy state and possible resolutions. The State Change Events tab shows the date and time when the health state changed. Also included on this tab are the important response times for the Web Application Monitor.



**Note:** To use the Summary Dashboard – Map view, you must use Windows PowerShell to configure Operations Manager with significant location-to-agent mapping. This is achieved by using the following example.

```
PS C:\> $Location = New-SCOMLocation -DisplayName "Seattle, WA" -Latitude 47.6063889
-Longitude -122.330833
PS C:\> $Agent = Get-SCOMAgent -Name "Server01.Contoso.com"
PS C:\> Set-SCOMLocation -Location $Location -Agent $Agent
```

More information about the Web Application Availability Monitoring template can be found at the following webpage:



#### Web Application Availability Monitoring Template

<http://go.microsoft.com/fwlink/?LinkId=321887>

## Guidelines for Configuring the Web Application Transaction Monitoring Management Pack Template

Using the Web Application Transaction Monitoring Management Pack template, you can create detailed web application monitoring using a Web Recorder for capturing web requests that you use as part of web application tests from specific geographical locations. The Web Application Transaction Monitoring Management Pack template differs from the Web Application Availability Monitoring Management Pack template in that each URL (or request) can be configured by using its own set of monitoring criteria. You use the Web Application Transaction Monitoring Management Pack template in scenarios in which advanced monitoring of web applications is required.

**The Web Application Transaction Monitoring Management Pack template configures the following:**

- Web address
- Watcher node
- Advanced monitoring:
  - Record a browser session
  - Edit request properties
  - Add performance counters

The Web Application Transaction Monitoring Management Pack template is configured by using the Add Monitoring Wizard. The following table describes each page of the Add Monitoring Wizard used to configure the Web Application Transaction Monitoring Management Pack template, including the available settings.

| Add Monitoring Wizard page used to configure the Web Application Transaction Monitoring Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                                               | Add a descriptive name for the monitor, and select or create a new Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Web Address                                                                                                      | Select the URL type, such as HTTP or HTTPS, and then add a single URL. Click the Test button to test access to the URL from the Management Server. Typically, this is the first URL in a series of URLs to be tested when you use the Web Application Transaction Monitoring Management Pack template. When the test is complete, you can click the Details button to display the details, such as the DNS Resolution Time and Total Response Time. You can also view the HTTP Request and HTTP Response details, which can help you troubleshoot connection issues if the test fails. |
| Watcher Node                                                                                                     | Select the agent-managed computers that you will use to test the web application. Remember that the watcher nodes should be the locations from which the web application is tested. You also specify the frequency of the tests by setting the Run This Query Every option. By default, the query is run every two minutes.                                                                                                                                                                                                                                                            |
| Summary                                                                                                          | A summary of the confirmed settings is displayed. You can confirm the settings, and then either create the monitor or go back through the wizard and make changes. The Configure Advanced Monitoring Or Record A Browser Session check box can be selected here. This option opens the Web Application Editor. The monitor is still created at this point, although you can edit it by using this option.                                                                                                                                                                              |

## **Editing the Web Application Transaction Monitoring Monitor By Using the Web Application Editor**

When you select the Configure Advanced Monitoring Or Record A Browser session check box, in the Web Application Editor, you can configure advanced settings for the monitor. Some more common settings that you can use are described in the following sections.

### **Start Capture**

The Start Capture option opens Microsoft Internet Explorer. You then browse to the web application as if you are an end user who is using the application. You open the web application (by logging on, if required) and browse through the webpages. You then perform the actions that a typical end user performs. When you do this, each request, including data that is inserted into each webpage, is recorded. When you click Stop Capture, the recorded requests are automatically inserted into the Web Application Editor where they can be edited. This process will save you time when you configure the web application tests, because you can browse to the web application. Then you can use the web application in the typical manner instead of manually entering each URL into the editor.

### **Request Properties**

Select a single request and then click Properties to open the Request Properties window. Here you can edit several settings, including URL, HTTP Method, and HTTP Version. You can also add, edit, or remove HTTP headers, which can be helpful when editing the requests for different environments. For example, you can edit the Accept-Language header and use a different language setting. On the Performance Counter tab, you select the performance counters that should be collected for the request, including several performance counters for the Base Page, Links, Resources, and Total. On the Monitoring tab, you configure monitoring options, such as Process Request Response Body. This option can be used when you want to monitor for specific text that is returned in the request. You can also use the Custom Error and Custom Warning tabs to configure custom monitoring of health states based on specific criteria. For example, when monitoring DNS resolution times, you can add Custom Warning criteria. By doing this, the monitor will change to a Warning health state when the DNS Resolution Time is greater than five seconds.

### **Configure Settings**

When you click the Configure Settings option, the Web Application Properties window opens. Here, you can configure global settings for the web application monitor, including authentication settings such as the Authentication Method, which is useful when you monitor web applications that require authentication. You can select an Authentication Method of None, Basic, Digest, Negotiate, or NTLM. Then, you select the related User Account. The User Account is usually an Operations Manager Action account that is already configured. By choosing the related user account, the Operations Manager agent can authenticate with the web application. You can also configure Proxy Settings, including the authentication and user accounts, and performance counters that should be collected for the application. Performance counters selected here are collected for the whole application instead of for a specific request. You can also configure Error and Warning health status settings for the web application that are based on Transaction Response Time. This lets you know whether a test is taking longer than the specified threshold to complete, such as five seconds. When you set a Transaction Response Time of more than five seconds, when the response time exceeds five seconds, the health state of the monitor changes to Warning or Error.

### **Viewing Web Application Transaction Monitors**

You can view the health state for Web Application Transaction monitors by using the Web Application State view. This view is located in the Web Application Transaction Monitoring folder of the Monitoring pane. A health state is displayed for each watcher node and web application being monitored. By using this view, when the health state changes for a specific web application or watcher node, you can view the affected web applications immediately. By right-clicking an application or watcher node here, you can open the Performance View, where you can select related counters to build a graph. The graph shows the performance data that is collected for the application based on the selected watcher node. The Health

Explorer can also be opened from the Web Application State view, where you can view the monitor's health state. Alerts generated by Web Application Transaction monitors can be viewed in the Active Alerts view of the Monitoring pane.

More information about the Web Application Transaction Monitoring template can be found on the following webpage:

 **Web Application Transaction Monitoring Template**

<http://go.microsoft.com/fwlink/?LinkID=321888>

## Guidelines for Configuring the Windows Service Management Pack Template

Use the Windows Service Management Pack template to monitor a specified Windows Service that is running on an agent-managed Windows-based computer and the behavior of that service. For business-critical applications that rely on Windows Services, this template can be used to monitor the health and availability of those services, and to collect performance metrics. By collecting metrics, you can view resources used by the services, which helps you identify trends in application health.

You use the Add Monitoring Wizard to configure the Windows Service Management Pack template. The following table describes each page of the Add Monitoring Wizard that you use to configure the Windows Service Management Pack template, including available settings.

**The Windows Service Management Pack template provides:**

- Monitoring of Windows Services on agent-managed Windows-based computers
- Alerting when a monitored service has stopped
- Alerting when a monitored service utilizes more than a given amount of CPU and memory resources
- Collection of performance data for memory and CPU resource usage



| Add Monitoring Wizard page used to configure the Windows Service Management Pack template | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                                                                        | Specify a name for the monitor and optionally include a description. You also select or create a Management Pack in which the monitor will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Details                                                                           | Either manually type the name of the service to be monitored, or browse to a computer to select an installed service. This is useful when you need to monitor a service and you might not know the exact service name. You can select a computer on which you know the service is installed, and then browse and select the service to be monitored. You also specify the Targeted group of computers on which the service should be monitored. Optionally, you can enable the Monitor Only Automatic Services option. When this option is selected, only services that have a startup value of Automatic are monitored, meaning that services with a startup value of Manual or Disabled will not be monitored. |
| Performance Data                                                                          | Optionally, you can configure an alert to be generated when CPU or memory usage of the selected service exceeds a specified value. You can also configure Performance Counter Sampling values so that alerts are generated only when CPU or memory usage exceeds a specified value for a given length of time. This is particularly useful when you know that a service uses additional resources during a heavy load, such as a service used in a backup application. You can configure the Performance Counter Sampling values such that an alert is generated only if CPU and memory resources are exceeded for more than an hour, for example.                                                               |
| Summary                                                                                   | A summary of the configured settings is displayed. You can confirm the settings, and then either create the monitor or go back through the wizard to make changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

When the Windows Service monitor is created, you can monitor the health state for each monitored service in the Windows Service State view, which you access in the Windows Service And Process Monitoring folder in the Monitoring pane of the Operations console. For each monitored service, the State, Display Name, and Path are displayed in this view, allowing you to quickly determine which services are in a critical state.

You can right-click a service name to open other context-sensitive views, such as the Alert View, Health Explorer, or Performance View. The Performance View is useful when you need to view the resources used by the service over a given time period.

When a monitored service has been detected as stopped, a Windows Service Stopped alert is generated in the Active Alerts view in the Monitoring pane of the Operations console. The alert shows the computer and service that caused the alert to be generated. When opening the alert, you can view additional details, such as the Display Name and BinaryPathName, from the Alert Context tab. These details are useful for troubleshooting a failed service, because you can quickly determine which process the service is using and then review the process state on the monitored computer.

## Demonstration: Creating a Process Monitor by using the Process Monitoring Management Pack Template

In this demonstration you will learn how to create a Process Monitor by using the Process Monitoring Management Pack Template.

### Demonstration Steps

- To perform this task, use the computer and tool information in the following table.

| Location | Value                                      |
|----------|--------------------------------------------|
| Computer | <b>LON-MS1</b>                             |
| Tool     | <b>Operations Console</b>                  |
| Pane     | <b>Authoring\Management Pack Templates</b> |
| Template | <b>Process Monitoring</b>                  |

- Use the **Process Monitoring** Management Pack Template to create a process monitor with the following settings:
  - Name: **Demo**
  - Management Pack: **DinnerNow**
  - Process name: **Notepad.exe**
  - Targeted group: **All Windows Computers**
  - Running Processes: **Generate an alert if the process runs longer than the specified duration**
- Start **Notepad**.
- Review the **Demo** alert that is generated in the Operations console.

 **Note:** It can take up to 10 minutes for the **Demo** alert to appear.

**Question:** You have to monitor a web application by replaying several web requests from different locations. There are over 30 requests that must be tested from each location. You must reduce the administrative overhead when you create the monitor. Which Management Pack template should you use?

## Lesson 2

# Distributed Application Models

Operation Manager has the ability to show the health state of your business-critical applications graphically by using a *Distributed Application Diagram*. This diagram enables the application owners to view, at a glance, the overall health state of all components that make up the distributed application.

Many of the Microsoft Management Packs include an automatically-generated Distributed Application Diagram for the application that is being monitored, including Active Directory Domain Services (AD DS) and Microsoft Exchange. From within the diagram, operators can use the Health Explorer to view the state of all relevant monitors that are currently being run against the distributed application.

To create a Distributed Application Diagram, you need to understand what components constitute the distributed application and how they can be added to the Distributed Application Designer.

### Lesson Objectives

After completing this lesson, students will be able to:

- Obtain the information that is required to create a Distributed Application Diagram.
- Describe the Distributed Application Designer, including templates.
- Create a Distributed Application Diagram.
- View a Distributed Application Diagram.

### Guidelines for Gathering Information for the Distributed Application Diagram

The Distributed Application Diagram in Operations Manager is a key feature that you can use to view the health and availability of an application or service and its monitored components, including their health state, relationship with other components in the application or service, and the affect (health rollup) that an unhealthy component is having on other components within the application or service.

For many organizations, the Distributed Application Diagram view of an application or service is the only view needed in the Network

Operations Center, because it includes all components of the business-critical application or service, including the underlying networking infrastructure the application or service relies on.

Some Management Packs such as the Management Packs for AD DS and Exchange include a Distributed Application Diagram that automatically discovers the various components of the application, allowing you to not only view how each component is related, but also the current health state of each monitored component.

For applications that do not already have a Distributed Application Diagram, however, such as an internal line-of-business application, you can either use the Distributed Application Designer to manually create one or develop a Management Pack to dynamically create one. For the relevant components of an application to be displayed in a Distributed Application Diagram, they must first be discovered by

#### Information required to create a Distributed Application Diagram includes:

- Application information
- Application servers
- Servers running SQL Server
- Servers running IIS
- Networking infrastructure
- Security information
- End-user locations
- Tests to be performed
- Health state indicators

Operations Manager. For this reason, it is important that you understand and document each component that the application or service relies upon.

To facilitate this, you can create a spreadsheet that details all components of the application, including relevant application servers, networking infrastructure, and end-user locations. This spreadsheet (also known as an *onboarding document*) can then be used to ensure the relevant components are discovered and monitored in Operations Manager. This is important, because you might need to install additional Management Packs and create overrides for the applications being monitored. It is important to remember that until each component has been discovered by Operations Manager, that component will not be available to be included in a Distributed Application Diagram.

Although each application or service can differ greatly in the function each provides, you can create an onboarding document that covers all key components that should be monitored and included in the Distributed Application Diagram. The following table describes some of the typical information requested in an onboarding document, which is passed to the application or service owner to complete.

| Category                                                      | Information requested                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application information                                       | Provide the name and version of the application to be monitored, including any specific updates that have been applied. Also include the program directory of where the application is installed.                                                                                                                                                                                                                                                                                                                                                                                             |
| Application servers                                           | <p>Provide the following information for each application server that hosts a component of the application:</p> <ul style="list-style-type: none"> <li>• Fully Qualified Domain Name (FQDN)</li> <li>• IP Address</li> <li>• The application component that the server hosts</li> <li>• Operating system version, including any service pack.</li> <li>• Any services or processes that the application relies upon</li> <li>• Roles or features that the application relies upon</li> <li>• Any additional software that the application relies upon</li> </ul>                              |
| Servers running SQL Server                                    | <p>Provide the following information for each server running Microsoft SQL Server used by the application:</p> <ul style="list-style-type: none"> <li>• SQL Server version, including any service packs and update</li> <li>• The database and log file names, including location</li> <li>• Any SQL agent jobs that the application uses</li> <li>• FQDN</li> <li>• IP address</li> <li>• Operating system version, including any service packs</li> <li>• Roles or features that the application relies upon</li> <li>• Any additional software that the application relies upon</li> </ul> |
| Servers running Microsoft Internet Information Services (IIS) | <p>Provide the following information for each server running IIS used by the application:</p> <ul style="list-style-type: none"> <li>• IIS server version, including any updates</li> <li>• Website names, including location</li> </ul>                                                                                                                                                                                                                                                                                                                                                      |

| Category                                                     | Information requested                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                              | <ul style="list-style-type: none"> <li>• Application pool names</li> <li>• FQDN</li> <li>• IP address</li> <li>• Operating system version, including any service packs and updates</li> <li>• Roles or features that the application relies upon</li> <li>• Any additional software that the application relies upon</li> </ul>                                                                     |
| Networking infrastructure and dependent application services | Provide a list of the network infrastructure that the application relies upon, including any relevant IP addresses. Also provide a list of any dependent application services such as AD DS or DNS.                                                                                                                                                                                                 |
| End User Locations                                           | Provide the locations of where users of the application reside.                                                                                                                                                                                                                                                                                                                                     |
| Topology                                                     | Provide a topology diagram of the application, including all components that it relies upon and the network relationship between each component.                                                                                                                                                                                                                                                    |
| Security                                                     | Provide the security account credentials that will be used to monitor the various application components.                                                                                                                                                                                                                                                                                           |
| Tests                                                        | <p>Provide a list of tests that can be performed against the application to determine the application's performance and availability. Typical tests include:</p> <ul style="list-style-type: none"> <li>• Web transactions, including any form information that should be submitted</li> <li>• Databases that should be queried, including the query to be used</li> <li>• IP port query</li> </ul> |
| Health State indicators                                      | <p>Provide a list of indicators to determine the health state of the application. Indicators could include:</p> <ul style="list-style-type: none"> <li>• Event logs</li> <li>• Application logs</li> <li>• Performance counters</li> <li>• Services</li> <li>• Processes</li> </ul>                                                                                                                 |

The preceding table is by no means exhaustive but rather represents a list of information that should be provided by the application or service owner. This information will then help you determine what components should be discovered and monitored in Operations Manager before you create a Distributed Application Diagram for the application.

## Overview of the Distributed Application Designer

Before you create a Distributed Application Diagram, you should understand how to use the Distributed Application Designer. In some cases, you might be creating a Distributed Application Diagram for which there is already a template provided. In this case you would select the relevant template before opening the Distributed Application Designer. Templates help you create Distributed Application Diagrams by automatically populating the diagram with relevant component groups.

Described in the following table are the various elements that constitute a Distributed Application Diagram, which you create by using the Distributed Application Designer.

**The Distributed Application Designer includes the following elements:**

- Objects
- Component Groups
- Relationships
- Health Roll-up

You can use a template to automatically create component groups

| Distributed Application Designer element | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Objects                                  | <p><i>Objects</i> represent the discovered components of an application, such as a database or an ASP.NET application. By default (when using blank template), only the following object types are included:</p> <ul style="list-style-type: none"> <li>• Distributed Application Component</li> <li>• Service</li> </ul> <p>As you add additional components to the diagram, however, other object types become available. The Distributed Application Designer can display up to seven object types at the same time. If you need to display a different object type when seven are already displayed, you must replace an existing object type. When you select an object type, the discovered objects for the selected object type are displayed. These objects can then be dragged onto the Distributed Application Designer canvas, which will ultimately be displayed in the Distributed Application Diagram.</p> |
| Component Groups                         | <p>A <i>component group</i> is used to group discovered objects. For example, you can create a component group named Windows Server 2012 R2 Operating System and then add the discovered Windows Server 2012 R2 Operating System objects to this component group. Although objects can be mixed within a component group, generally they are used to group objects of one object type, such as SQL databases or IIS websites.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Relationships                            | <p><i>Relationships</i> in the Distributed Application Designer are used display how each component group is related to other component groups. However, when relationships are viewed in the Distributed Application Diagram, the health rollup of an application or service is not reflected.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Health Roll-up                           | <p>You can configure the health rollup for each component group created in the Distributed Application Designer. The Health Roll-Up element determines how the health of the distributed application is depicted when the health state of a component group changes. Health Roll-Up is discussed in more detail in the next topic.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Distributed Application Diagram Templates

When creating Distributed Application Diagrams, you can use predefined templates to assist with creating the relevant component groups. With System Center 2012 R2 Operations Manager, the following Distributed Application Diagram templates are included:

- **.NET 3-Tier Application.** The .NET 3-Tier Application template can be used in conjunction with the .NET Application Performance Monitoring Management Pack template to create Distributed Application Diagrams of monitored Microsoft .NET Framework web applications. Four component groups covering the Client Perspective, Presentation Tier, Business Tier, and Data Tier are provided with the template. This allows you to quickly configure the Distributed Application Diagram for components discovered by the Application Performance Monitoring Management Pack template.
- **Line of Business Web Application.** The Line of Business Web Application template can be used to quickly create a Distributed Application Diagram of a typical web farm. Included with the template are two component groups named Web Application Web Sites and Web Application Databases.
- **Messaging.** The Messaging template can be used to create a Distributed Application Diagram for a typical messaging environment and includes component groups for typical messaging infrastructure components such as Directory Services, Storage, Network Services, Physical Network, and Messaging Clients.
- **Blank.** The Blank template is used to create a Distributed Application template from scratch. This template is used when none of the default templates fit your Distributed Application Diagram requirements.

## The Process of Creating a Distributed Application Diagram

To create a Distributed Application Diagram, you use the Create a New Distributed Application task that is available from the Distributed Applications node in the Authoring pane of the Operations console. This opens the Distributed Application Designer, where you must first provide a name for the Distributed Application Diagram you are going to create. Optionally, you can include a description for the various components that are included in the Distributed Application Diagram. You must also select a template that the Distributed Application Diagram will be based on, such as Messaging or Blank. Finally, you must select or create an unsealed Management Pack in which the Distributed Application Diagram will be saved.

After supplying the name, template, and Management Pack for the Distributed Application Diagram, the Distributed Application Designer opens the canvas, where you can modify any existing component groups or add additional component groups.

### Adding Component Groups

If the blank template was selected, the canvas does not contain any component groups. Use the Add Component toolbar button to create a new component group. When creating a new component group, a Create New Component Group dialog box opens, where you first provide a name for the component group, such as Windows Server 2012 R2 Operating Systems. After providing a name for the component group, you must select the object type that will be used to group objects within the component group. You do this by clicking the Objects Of The Following Type(s) option, and then browsing the list of object types. It is important to remember that you are not selecting specific objects such as a database here, but rather the object type, such as database. The object types are split into eight separate sections as follows:

**Using the Distributed Application Designer, you can:**

- Create component groups that contain objects to be displayed in the Distributed Application Diagram
- Create relationships between component groups to show dependencies
- Configure health rollup to accurately show the application's health in the Distributed Application Diagram

- Administrative Item
- Collection
- Configuration Item
- Extension Base Class
- Extension Type Class
- Network Device (Pending)
- Network Discovery Server
- UNIX/Linux Supported Agents

For most scenarios, the object types that you will want to include in a component group will be located within a subgroup named Logical Entity, which is located within the Configuration Item section. The Logical Entity subgroup contains logical object types such as Operating System, Network Adapter, Perspective, Service, and Computer Role. There are many subgroups within the Logical Entity subgroup that further define the object types. For example, to select the Windows Server 2012 R2 Operating System object type for the component group, you browse through the object types as follows:

`Object\Configuration Item\Logical Entity\Operating System\Windows Operating System\Windows Server Operating System\Windows Server 2012 Operating System\Windows Server 2012 R2 Operating System\Windows Server 2012 R2 Full Operating System.`

By selecting the object types you determine which objects can be added to a component group. After selecting the object type, such as Windows Server 2012 R2 Full Operating System, and clicking OK in the Create New Component Group dialog box, the Objects pane within the Distributed Application Designer updates to show the discovered Windows Server 2012 R2 Full Operating Systems. You then add to the component group the relevant operating systems that should be included in the Distributed Application Diagram. You can drag the objects to the component group, or you can right-click an object and then click Add To display a list of available component groups to which the selected object can be added. You then click the component group, and the object is added to it.

As you build out your Distributed Application Diagram, you add multiple component groups for each component that should be monitored in the application.

### **Creating Relationships Between Component Groups**

After you create the component group for each component in the application that will be monitored, and you add the relevant objects to the component group, you can then configure the relationship between the component groups. Doing so displays each component's dependencies in the diagram view, as described in the next topic. To create a relationship between two components, where the first component group is dependent on the second component group, on the toolbar, click the Create Relationship button, and then drag the first component group to the second component group. Suppose you were creating a Distributed Application Diagram for a web application that uses a database hosted on a server running SQL Server. In the Distributed Application Diagram, you could create two component groups named Web Sites and Web Site Databases. You would then add the relevant website to the Web Site component group, and add the relevant database to the Web Site Databases component group. Finally, you would create a relationship between the Web Sites component group and then Web Site Databases component group.

In the Distributed Application Diagram, a dotted line between the component groups is displayed, with the arrowhead pointing to the Web Application component group. This shows that the website is dependent on the database. You can add multiple relationships to and from multiple component groups. For example, you might want to add a component group named IIS Server Role, and then add a relationship between the Web Sites component group and the IIS Server Role component group to show that the website also depends on the IIS Server Role.

## Configuring Component Group Health Roll-Up

After you have saved the Distributed Application Diagram by clicking the Save button, you can configure the health roll-up for each component group. This determines the health state of the component group and overall Distributed Application Diagram based on one of three possible rollup algorithms: the best health state of any member, the worst health state of any member, and the worst state of a percentage of members in good health state. To understand how this works, consider the following example. You have a web server farm that contains four web servers. You create a component group named Web Server Farm, and add the four web servers to it. Note the effect when you configure the following:

- **Health rollup of the Web Server Farm component group to use the Best Health State of Any Member.** If any web server in the component group is healthy, the component group is healthy. If all web servers in the component group are unhealthy, the component group is unhealthy.
- **Health rollup of the Web Server Farm component group to use the Worst Health State of Any Member.** If any web server in the component group is unhealthy, the component group is unhealthy.
- **Health rollup of the Web Server Farm component group to use the Worst State of A Percentage Of Members In Good Health State.** When using this algorithm, you must also specify a percentage. If you set a percentage of 50 percent, for example, if more than two of the four web servers are unhealthy, the component group is unhealthy.

You can configure the health rollup algorithm for the Availability, Configuration, Performance, and Security entities. By configuring the health rollup algorithm for each component group in the Distributed Application Designer, you can control how the health of the application is displayed when viewing it in the Distributed Application Diagram.

For more information about configuring Distributed Application Diagrams in Operations Manager visit the following website.

### **Distributed Applications**

<http://go.microsoft.com/fwlink/?LinkId=404089>

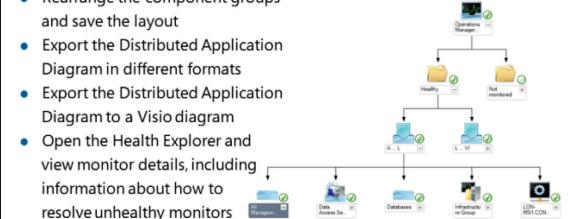
## Process of Viewing Distributed Application Diagrams

After you save the Distributed Application Diagram, you can open it from within the Distributed Applications view in the Monitoring pane of the Operations console. You can open the Diagram view in two ways: right-click a Distributed Application, click Open, and then click Diagram View; or select the Distributed Application Diagram and then use the Diagram View task. When opened, the Diagram view displays each component group added when the Distributed Application Diagram was created. Relationships that were configured between component groups

are displayed as a blue dotted line with an arrowhead pointing to the dependent component group. By default, each component group is collapsed, but you can expand the component group to view the objects that it contains by clicking the Plus Sign. Expanding the component group displays the health state of each object contained in the Diagram view and also the health state of each component group in the distributed application, so you can quickly determine whether any component group or object is in an unhealthy state.

### When viewing a Distributed Application Diagram, you can:

- Expand component groups and view health state information for each monitored object
- Rearrange the component groups and save the layout
- Export the Distributed Application Diagram in different formats
- Export the Distributed Application Diagram to a Visio diagram
- Open the Health Explorer and view monitor details, including information about how to resolve unhealthy monitors



When you expand a component group and then select an object within it, the Detail view displays information about the selected object. For example, if a Windows Server 2012 R2 Full Operating System object is selected, the Detail views display information such as Operating System Version, Build Number, Service Pack Version, System Drive, Windows Directory, Physical Memory (MB), and Logical Processors. This information can be useful when troubleshooting an object that is in a critical health state, because you can view key properties of the object in question, and you can correlate this information to other entities related to the object, such as performance counters, alerts, and events.

The component groups within the Diagram view can be rearranged so that they are displayed in a more logical manner based on the topology of the application being monitored. For example, you can drag component groups around the view and also use the Layout Direction toolbar feature to change the layout of all component groups. This is useful when there are a large number of component groups in the diagram. When changing the layout of component groups in the diagram, you can click the Save button to save the current layout. This ensures the layout is retained when you close the Distributed Application Diagram and then reopen it.

Other useful toolbar features include:

- **Print.** You can print a paper copy of the Distributed Application Diagram.
- **Zoom.** You can zoom in and out, which is useful when a Distributed Application Diagram contains many component groups and you need to focus on a particular area.
- **Filter By Health.** You can use this feature to filter component groups and objects based on health state such as Green (healthy), Yellow (warning), and Red (critical). This is useful when you need to filter all objects that are in a critical health state.
- **Export Configuration.** The Export Configuration feature can be used to create an image of the Distributed Application Diagram in the JPEG (.jpg), bitmap (.bmp), or Portable Network Graphics (.png) file format. This is useful when you need to show the Distributed Application Diagram to people who do not have access to the Operations console. You can export the image and then include it in an email, for example, or make it available on a network file share.
- **Export Page to Visio.** The Export Page to Visio feature can be used to create a Visio diagram of the Distributed Application Diagram. This is useful when you need to create a topology diagram of the application, because each component group and the objects it contains can then be loaded into a Visio diagram and worked on.

### Health Explorer

For each component group and the objects that it contains, you can open the Health Explorer by right-clicking the component and then clicking Health Explorer, which displays all monitors used to gather the component's health and availability information. By default, only unhealthy child monitors are displayed in the Health Explorer, but you can remove the scope to display all monitors. The Health Explorer is particularly useful when troubleshooting unhealthy objects, because the unhealthy monitors and knowledge about the monitor, including a summary of what the monitor is monitoring, possible causes for the unhealthy monitor, and resolutions to help fix the monitor are displayed. You can also use the State Change Events tab to determine when the monitor changed from a healthy to an unhealthy state. This is useful, because you can correlate this information with other events and alerts that have occurred within the environment. You can also view the properties of a selected monitor and override the monitor from within the Health Explorer. You might want to do this when you need to modify the threshold of a monitor you know should not be generating an unhealthy state.

## Demonstration: Creating a Distributed Application Diagram

In this demonstration, you will learn how to create a Distributed Application Diagram.

## Demonstration Steps

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Console</b>       |
| Pane     | <b>Authoring</b>                |
| View     | <b>Distributed Applications</b> |

2. Use the **Create a New Distributed Application** task to create a new Distributed Application Diagram with the following settings (leave all other default settings):
  - Name: **DinnerNow**
  - Template: **Line of Business Web Application**
  - Management Pack: **DinnerNow**.
3. From the **Database** pane, add the **DinnerNow** database to the **DinnerNow Web Application Databases** component group
4. From the **Web Site** pane, add the **Default Web Site** for LON-AP2 to the **DinnerNow Web Application Web Sites** component group
5. Close the Distributed Application Designer without saving the changes.

**Question:** You are creating a Distributed Application Diagram for an in-house line-of-business application. You attempt to add the website to a new component group you created in the Distributed Application Designer, but the website is not displayed. What could be the problem?

## Lesson 3

# Global Service Monitor

When configuring synthetic transactions to monitor web applications, it is important to include monitoring from each location where application users reside. In many cases, users of the application might not reside in your internal network and instead access the public-facing part of the application from an Internet-based location. In this scenario, you can use Global Service Monitor to monitor public-facing web applications from external locations hosted in Microsoft Azure.

It is important to understand how Global Service Monitor is configured in Operations Manager so that you can achieve monitoring from both internally-based and externally-based locations.

### Lesson Objectives

After completing this lesson, students will be able to:

- Describe the purpose of Global Service Monitor.
- Configure Global Service Monitor.
- View the information collected from Global Service Monitor.

### Overview of Global Service Monitor

Global Service Monitor is a new feature introduced with System Center 2012 Service Pack 1 (SP1) Operations Manager and is available to customers who purchase System Center with Software Assurance. You can use this feature to monitor external-facing web applications from the cloud (more specifically, Microsoft Azure). This service helps organizations monitor the performance of their external-facing applications from outside their datacenter. Traditionally, this has been very difficult to do without placing resources outside the organization.

#### **Global Service Monitor integrates with System Center 2012 R2 Operations Manager to provide:**

- Web Application Availability monitoring for externally facing web applications
- Monitoring from Windows Azure in over 15 locations around the world
- Integration with the Web Application Availability Monitoring Management Pack template and the Web Application Transaction Monitoring Management Pack template
- Performance and availability information that is viewed in the same way as it is for internal web applications

Global Service Monitoring allows you to take advantage of the Microsoft Azure infrastructure by using watcher nodes that are distributed throughout the globe to monitor the external-facing web applications. Then you can monitor the performance and availability of the web application from locations around the world. Global Service Monitoring integrates with Operations Manager by using several Management Packs. The Management Packs are imported into the Management Group, and then built on the Web Application Availability Monitoring Management Pack template and the Web Application Transaction Monitoring Management Pack template.

After you register and install the related Management Packs for Global Service Monitor, you can configure the Web Application Availability Monitoring Management Pack template. This is the same process as when you monitor intranet applications.

When you configure Global Service Monitoring for web applications, the following 15 locations are currently available in Microsoft Azure:

- Australia: Sydney
- Brazil: Sao Paulo

- Europe: Amsterdam, London, Paris, Stockholm, Zurich
- Russia: Moscow
- Singapore
- Taipei
- United States: Chicago, Los Angeles, Miami, Newark, San Antonio

## The Process of Configuring Global Service Monitor

Before you can configure Global Service Monitoring in Operations Manager, the following prerequisites must be met:

- **Internet access.** The Management Servers in the resource pool that you use for Global Service Monitor must have access to the Internet so that they can communicate with agents running in Microsoft Azure. You do not need to deploy any agents, however, because these are already available in Microsoft Azure. From a security perspective (and as a best practice), you should create a new resource pool that will host the Management Servers that require Internet access unless the Management Servers you plan to use with Global Service Monitor already have Internet access.
- **Windows Identity Foundation (WIF).** You must install WIF on the Management Servers that will be communicating with Microsoft Azure. You must also install WIF on all computers that host the Operations Manager console.
- **Global Service Monitor Subscription.** You must have an existing subscription to Global Service Monitor.

You can obtain a three-month trial subscription by going to the following link.



<http://go.microsoft.com/fwlink/?LinkId=391274>

After you register, you will receive a Global Service Monitor ID and a download link to the Global Service Monitor Management Packs that must be installed in Operations Manager.

- **Configuring Global Server Monitor.** After you subscribe to the Global Service Monitor and you receive your Global Service Monitor ID, you must install the Global Service Monitor Management Packs. Optionally, if you want to download the web test results created by Global Service Monitor so that you can attach them to alerts in Operations Manager and forward them as work items in TFS, you must also install and configure the Alert Attachment Management Pack and the TFS Work Item Synchronization Management Pack.

You can also download the Global Service Monitoring Management Packs from the Microsoft Download Center at the following link:



**System Center Global Service Monitor Management Packs**

<http://go.microsoft.com/fwlink/?LinkId=391275>

### Before configuring Global Service Monitor:

1. Create a resource pool that includes the Management Servers that will connect to the Global Service Monitor service
2. Ensure the Management Servers have Internet access
3. Install Windows Identity Foundation on the Management Servers and computers running the Operations console
4. Subscribe to Global Service Monitor and install the Global Service Monitor Management Packs

### When configuring Global Service Monitor:

1. Create web application availability tests
2. Create Visual Studio web tests

After you have installed the Global Service Monitor Management Packs, a new node named Global Service Monitor becomes available in the Administration pane of the Operations console. From here, you can use the Start Subscription link to connect to Microsoft Azure and start the Global Service Monitor subscription. Note that if you have not already installed WIF, the Start Subscription link will not be available. Instead, you must click the Install Windows Identity Foundation link to install it. After the installation has completed, you must navigate away from the Global Service Monitoring node and then return to the Global Service Monitoring node for the Start Subscription link to be displayed.

After you click the Start Subscription link, a Start Global Service Monitor wizard starts. The following table describes each page of the Start Global Service Monitor wizard.

| Start Global Service Monitor wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subscription Credentials                 | Supply the subscription ID and organization details that were used when creating the Global Service Monitor subscription.                                                                                                                                                                                                                                                                                                                                                           |
| Component Configuration                  | Specify the resource pool that should be used to connect to the Global Service Monitor service. If the Management Servers access the Internet by using a proxy server, Proxy server information can also be included on this page by selecting the Use Proxy Server To Connect option. For authentication with the proxy server, you must create a Run As account that has the relevant permissions and then configure the Global Service Monitor Run As Profile with this account. |
| Summary                                  | Review the configured settings, and optionally go back through the wizard to make changes before clicking the Start Subscription button.                                                                                                                                                                                                                                                                                                                                            |

After completing the Start Global Service Monitor wizard, the subscription is activated, and you can start using it to monitor your externally-facing websites from the cloud.

### Creating Web Application Availability Tests

To create a web application availability test and test a web application from the cloud, you use the Configure Web Application Availability Tests link that is available in the Global Service Monitor node in the Administration pane of the Operations console. This opens the Web Application Availability Management Pack template with the Add Monitoring Wizard, as described in the topic “Guidelines for Configuring the Web Application Availability Monitoring Management Pack Template” earlier in this module. You configure the template in exactly the same manner, except on the Where To Monitor From page, an additional section named External Locations is available. In this section, you can click Add and then select the external locations you want Global Service Monitor to monitor your web application from. You can also include internal locations as usual, which is useful when you want to compare how a web application performs locally versus externally. While working through the Add Monitoring Wizard, on the View And Validate Tests page, use the Change Configuration button to ensure relevant frequency, performance collection, and alerts are configured appropriately.

### Creating Visual Studio Web Tests

A new Management Packs Template named Visual Studio Web Test Monitoring is added to Operations Manager after you install the Global Service Monitor Management Packs. This template provides the ability to run authenticated, multistep web tests against a web application, and uses .web test files created in Microsoft Visual Studio by using the Web Test Recorder. Using Visual Studio to create .web test files for use in Global Service Monitor provides much more detailed control over what is monitored in a web application. For example, users might need to log on to the web application, browse through multiple

websites, and add items to a shopping cart. Using Visual Studio Web Tests, Global Service Monitor can record these actions and then replayed by using from location around the world. Additionally the web test results can also be collected and attached to alerts in Operations Manager, which can then be assigned to engineers in TFS Work Items.

To create a Visual Studio web test, you use the Configure Visual Studio Web Tests link available in the Global Service Monitoring node in the Administration pane of the Operations console. Clicking this link opens the Visual Studio Web Test Monitoring Management Pack template and the Add Monitoring Wizard. Described in the following table are the pages of the Add Monitoring Wizard when used with the Visual Studio Web Test Monitoring Management Pack template, including the settings configured on each page.

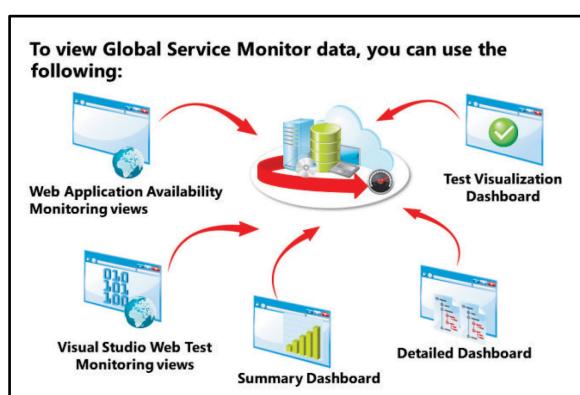
| Add Monitoring Wizard page used to configure the Visual Studio Web Test Monitoring Management Pack template | Description                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General                                                                                                     | Supply a descriptive name for the web test and, optionally, a description. You must also select or create an unsealed Management Pack in which the web test will be saved. |
| What To Monitor                                                                                             | Add the .web test files that were created in Visual Studio.                                                                                                                |
| Where To Monitor From                                                                                       | Add the external locations that Global Service Monitor should monitor from.                                                                                                |
| View and Configure Tests                                                                                    | View the tests that will be performed by Global Service Monitor, and then configure the frequency, performance collection, and alerting options.                           |
| Summary                                                                                                     | Review the settings that have been configured and, optionally, go back through the wizard to make any changes before clicking the Create button.                           |

After you have created the Visual Studio Test Monitor, Global Service Monitoring starts monitoring the defined web application with the Visual Studio tests that you supplied.

## The Process of Viewing Global Service Monitor Data in the Operations Manager Console

After you configure Global Service Monitor and create either Web Application Availability tests or Visual Studio Web Tests, you can view monitoring information relating to them in both the Global Service Monitoring node in the Administration pane, and you can access various views in the Monitoring pane.

For each web application that is being monitored by Global Service Monitor, you can use the Web Application Status view, which is located in the Application Monitoring\Web Application Availability Monitoring folder, in the Monitoring pane of the Operations console. The health state for each web application is displayed here and is useful



in obtaining an up-to-date view of a web application's health state. Other views in this folder include the Active Alerts view, where any associated alerts that have been generated for web applications will be displayed. The Test State view can also be used to view the health state of all web tests being performed by Global Service Monitor.

You can also view any active alerts by selecting the View Active Alerts link in the Global Service Monitoring node in the Administration pane, in the Web Application Availability Test Actions section. From here, you can also open the Test State pane by clicking the View Test State Link, which displays information relating to the individual URLs and locations being tested.

To view test information and alerts that have been generated by Visual Studio web tests, you can use the Test State, Web Application Status, and Active Alerts views that are located in Application Monitoring\Visual Studio Web Test Monitoring in the Monitoring pane. From the Visual Studio Web Test Status view, you can open the Health Explorer for a selected web application and then view the monitors, including their health state. This is useful when troubleshooting an application that is in an unhealthy state, because you can quickly determine which monitors are unhealthy and target your troubleshooting more accurately.

In the Global Server Monitoring node, in the Administration pane, you can use the Visual Studio Web Tests Actions section to open the Active Alerts pane and view any active alerts relating to web application that is being monitored by Visual Studio web tests. You can also click the View Test State link from here, which opens the Test State pane. This pane displays individual tests that are being performed, and includes the web application's health state and the locations from which the tests are being performed.

### **Dashboard Views**

There are a number of dashboard views in Operations Manager that can be used to obtain useful information about the monitoring performed by Global Service Monitor. These views are described in the sections that follow.

#### ***Summary Dashboard***

The Summary Dashboard can be used to check application availability from each location that is being monitored by Global Service Monitor. Included in the dashboard is a world map, which displays each location where monitoring is being performed and a roll-up of the health state in each location. When selecting a location in the dashboard, Test Status information is displayed that includes the test names, transaction response times, and sample times. This status information is useful because you can select multiple locations and then compare their data, for example, you can compare the transaction response times for each location. You can open the Summary Dashboard by clicking the Summary Dashboard task that is available when you click the View Test State link in the Global Service Monitor node of the Administration pane. By clicking a test in the Summary Dashboard, you can then use the Detailed Dashboard – List task that becomes available in the Tasks pane.

#### ***Detailed Dashboard***

When you need to investigate a test or alert, for any tests that are being performed by using the Web Application Availability Monitoring web tests, you can open the Detailed Dashboard from the Tasks pane. In this dashboard, you select a location and test to investigate, which then displays six performance metrics, including Total Transaction Time, Time To First Byte, Content Time, and DNS Resolution Time. Additionally, you can select multiple locations and compare how the tests performed at each location. This is useful because you can compare DNS Resolution Times from multiple locations, for example, when you suspect a certain location is experiencing a problem resolving a web applications URL.

#### ***Test Visualization Dashboard***

The Test Visualization Dashboard can be used to display results from Global Service Monitor web tests in a view similar to that in Visual Studio. For each test result, you can view the Transaction Response Time in seconds and the sample time. You can also open the Detailed Dashboard from here by clicking a test and then using the Detailed Dashboard – List task.

Using a combination of the views and dashboards described in this topic, you can quickly determine the health state of monitored web applications from locations around the world, and obtain detailed information to help troubleshoot web applications when they are in an unhealthy state.

Verify the correctness of the statement by placing a mark in the column to the right.

| Statement                                                         | Answer |
|-------------------------------------------------------------------|--------|
| You do not need Operations Manager to use Global Service Monitor. |        |

## Lesson 4

# Real-Time Visio Dashboards

By using the Visio 2010 add-in for System Center 2012 Operations Manager, you can take customized dashboards created in the add-in and display them in Microsoft SharePoint websites. These dashboards are updated automatically and provide a real-time view of the health and availability of components in your monitored environment. There are a number of tasks that must be performed before these Visio dashboards can be made available in SharePoint, so it is important that you understand how to complete them.

### Lesson Objectives

After completing this lesson, students will be able to:

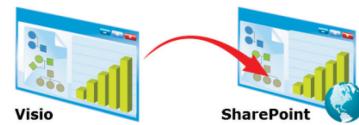
- Install and configure the Visio 2010 add-in.
- View a Distributed Application Diagram in Visio 2010.
- Publish a Visio diagram and create a monitoring dashboard by using the Visio web part.

### The Process of Installing the Visio 2010 Add-In and SharePoint 2010 Visio Services Data Provider

You can display an up-to-date view of an environment by using the Visio 2010 add-in for System Center 2012 Operations Manager to create a Visio diagram and link objects in Operations Manager. For example, you could create a Visio diagram of your datacenter and include shapes for file servers, email servers, and various networking infrastructure elements. Using the Visio 2010 add-in, you can then link these shapes to the discovered objects in Operations Manager. The Visio diagram then shows the health state of these objects in real-time. As the health state of these objects change in Operations Manager, the Visio diagram automatically refreshes to show the updates.

**The Visio 2010 add-in and SharePoint 2010 Visio Services Data Provider provide the ability to:**

- Link Visio shapes to Operations Manager objects
- Update the health state of linked objects in Visio
- Import a Distributed Application Diagram from Operations Manager and display an updated view of its health state
- Publish customized dashboards created in Visio to SharePoint websites



In addition, Distributed Application Diagrams that you create in Operations Manager can be exported in Visio format and then loaded into Visio. Visio then automatically connects to the Operations Manager Management Server and updates the objects' health state in Visio automatically.

With the SharePoint 2010 Visio Services Data Provider, you can publish customized dashboards created in Visio to SharePoint websites. As the health states of objects change, the SharePoint website automatically updates to reflect the new health state.

#### Installing the Visio 2010 Add-in

Before you install the Visio 2010 add-in, the following prerequisite software must be installed:

- Visio 2010 Professional or Premium
- System Center 2012 Operations Manager Operations console or Operations Manager 2007 Authoring console
- SP.NET Framework 3.5 SP1

You can download the Visio 2010 and SharePoint 2010 Extensions for System Center 2012 from the Microsoft Download Center.



### **Microsoft Visio 2010 and SharePoint 2010 Extensions for System Center 2012**

<http://go.microsoft.com/fwlink/?LinkId=391276>

After downloading and extracting the zip file, a folder named Visio 2010 And SharePoint 2010 Extensions For System Center 2012 is created and contains the following subfolders:

- **Client.** Contains the x64 and x86 versions of the Visio 2010 add-in
- **Docs.** Contains documentation for installing and using the Visio 2010 add-in and SharePoint Data Provider
- **Server.** Contains the SharePoint 2010 Data Provider software

To install the Visio 2010 add-in, you run OpsMgrAddinSetup.msi from either the x64 or x86 folder in the Client folder. This opens the Visio add-in for System Center 2012 – Operations Manager Wizard. You can optionally change the installation location during the wizard, but generally all default settings should be accepted. After the wizard completes, the Visio 2010 add-in is installed. To confirm the Visio 2010 add-in was successfully installed, you can open Blank drawing in Visio, and a new group on the ribbon named Operations Manager will be displayed.

### **Installing the SharePoint 2010 Visio Services Data Provider**

Before you install the SharePoint 2010 Visio Services Data Provider, the following prerequisite software must be installed first:

- System Center 2012 – Operations Manager Operations console or Operations Manager 2007 Authoring console
- SharePoint 2010 Enterprise
- .NET Framework 3.5 SP1

To install the SharePoint 2010 Visio Services Data Provider, you first run OpsMgrDataModule.msi from the Server folder. This opens the Visio Services Data Provider for System Center 2012 – Operations Manager Setup Wizard. You can optionally change the installation location during the wizard, but generally all default settings should be accepted. After the wizard completes, you must open the SharePoint 2010 Management Shell as an administrator, and then browse to the folder where the SharePoint 2010 Visio Services Data Provider was installed. By default this is C:\Program Files\Visio Services Data Provider for System Center 2012 – Operations Manager. You then run the following cmdlet:

**\InstallOpsMgrDataModule.ps1.** Note that the SharePoint Administration Service must be running before you run this cmdlet.

After the cmdlet has completed, you can confirm that the Visio Services Data Provider for System Center 2012 – Operations Manager was installed successfully by running the following cmdlet: **Get-SPSolution**.

The Opsmgrdatamodule.wsp module should be displayed with the Deployed status of True. Note that it can take up to 15 minutes for the module to be deployed to the SharePoint farm.

## The Process of Viewing Distributed Application Diagrams in Visio 2010

One of the most powerful features of the Visio 2010 add-in for Operations Manager is the ability to create a Visio diagram based on an Operations Manager Distributed Application Diagram. This diagram allows you to instantly represent your applications and services monitored by Operations Manager in a Visio diagram. In addition, you can include other shapes in the Visio diagram and link them to objects in Operations Manager. Before you can import and use a Distributed Application Diagram in Visio, you must first configure the Operations Manager Data Source, as described in the steps that follow.

**To view a Distributed Application Diagram in Visio, you must:**

- Configure the Operations Manager Data Source in Visio
- Export a Distributed Application Diagram from Operation Manager in Visio file format
- Open the Visio diagram in Visio

### Configuring the Operations Manager Data Source in Visio

To configure the Operations Manager Data Source in Visio, perform the following steps:

1. Open Visio, and then on the **Choose a Template** page, open a **Blank** drawing.
2. On the ribbon, click the **Operations Manager** tab, and then click **Configure**.
3. In the **Configure Data Source** dialog box that opens, type the following:
  - **Management Server Computer Name**
  - **Operations Manager Web Console URL**
4. Optionally, click the **Automatically refresh data** option to have the Visio diagram updated automatically.
5. Click **OK** to save the configuration.

After you configure the Operations Manager Data Source in Visio, you can import a Visio diagram created in Operations Manager, as described in the next set of steps.

### Viewing a Distributed Application Diagram in Visio

To view a Distributed Application Diagram in Visio, perform the following steps:

1. In the Operations console, open the **Diagram View** for the Distributed Application Diagram.
2. Expand the component group to display the level of detail you want to include in the Visio diagram.
3. Use the **Export Page to Visio** option on the toolbar to export the Distributed Application Diagram as a Visio (.vdx) file.
4. Save the file to a location accessible from the computer running Visio.
5. Open Visio, and then open the Visio file created in step 3.

After opening the Visio diagram, Visio connects to the Management Server to obtain the latest health state for each Operations Manager object in the diagram.

You can use the Add Status button on the ribbon to add a Status legend to the diagram. This is useful for viewing the status of the connection to Operations Manager, including the last refresh time.

## The Process of Publishing the Visio Diagram to SharePoint and creating a Monitoring Dashboard

After importing a Distributed Application Diagram from Operations Manager into Visio, you can publish the diagram to SharePoint and make it available in a SharePoint webpage. You might do this if you wanted to make Distributed Application Diagrams available to users who do not have access to the Operations console but still need to see how an application or service is performing.

### Publishing a Visio Diagram to SharePoint

To publish a Visio diagram to SharePoint, you must perform the following steps:

1. Open the diagram in Visio.
2. On the **File** menu, click **Save & Send**.
3. In the **Save & Send** dialog box, click **Save to SharePoint**.
4. Ensure that under **File Types**, the **Web Drawing** option is selected.
5. Either click **SharePoint Location** or click **Browse for the Location of the Shared Documents library in SharePoint**.
6. Click **Save As**, and then specify the name and location where the file should be saved in SharePoint.
7. Click **Save**.

The Visio diagram is then published to SharePoint in the specified location. The SharePoint 2010 Visio Services Data Provider ensures that the most current data is obtained from the Operations Manager Management Server.

### Creating a Monitoring Dashboard in SharePoint

Using the Visio Web Services Web Part, you can create a monitoring dashboard in SharePoint that uses a published Visio diagram, such as a Distributed Application Diagram from Operations Manager. To create a monitoring dashboard in SharePoint, perform the following steps:

1. In SharePoint, browse to the **Shared Documents** library.
2. From **Site Actions**, click **More Options**.
3. Select the web part, and then click **Create**.
4. Provide a name for the new page.
5. In the **Layout** section, select **Header**, **Right Column**, and **Body**.
6. Click **Create** to create the webpage.
7. On the **Insert** tab, click **Web Part**.
8. In the **Categories** list, click **Office Client Applications**, and then in the **Web Parts** list, click **Visio Web Access**.
9. Click **Add**.
10. Edit the web part.

#### Using the SharePoint 2010 Visio Services Data Provider, you can:

- Publish a Visio diagram, such as a Distributed Application Diagram, to SharePoint
- Create a Monitoring Dashboard in SharePoint that includes the published Visio diagram
- Connect the SharePoint 2010 Visio Services Data Provider to the Management Server to retrieve status updates

11. Next to the **Web Drawing URL** property, click **Browse**, and then browse to and select the published Visio diagram.
12. Configure the **Automatic Refresh** property. The minimum supported value is 1 minute.
13. Clear the **Show Open in Visio** check box.
14. Click **OK** to save the webpage.

The webpage displays the Visio diagram, including an updated view of the Distributed Application Diagram.

**Question:** What must be installed to use the Visio 2010 add-in?

# Lab: Configuring End-to-End Service Monitoring

## Scenario

Contoso, Ltd. has several internally-facing line-of-business applications that the staff uses to perform daily tasks. It is critical that these applications be available at all times. Many of the applications are reliant on other components such as computers hosting SQL Server and IIS Server, including the networking infrastructure. To enable monitoring of these business-critical applications, you must configure end-to-end monitoring for them.

## Objectives

After completing this lab, students will be able to:

- Configure agent locations for the Summary Dashboard
- Configure synthetic transactions by using Management Pack templates.
- Create a Distributed Application Diagram.
- Create a Visio diagram for the distributed application.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machines:** 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-MS2, 10964C-LON-AP2; 10964C-LON-SC1

**User Name:** Contoso\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, in Hyper-V Manager, click **10964C-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Contoso**
5. Repeat steps 2–4 for the following virtual machines:
  - 10964C-LON-SQ1 (On LON-HOST1)
  - 10964C-LON-MS1 (On LON-HOST2)
  - 10964C-LON-MS2 (On LON-HOST1)
  - 10964C-LON-AP2 (On LON-HOST2)
  - 10964C-LON-SC1 (On LON-HOST2)



**Note:** Before you start this lab, make sure that all Windows Services that are set to start automatically are running. The exception is for the .NET Framework NGEN v4.0.30319\_X86 and .NET Framework NGEN v4.0.30319\_X64 services because these services stop automatically when they are not being used.

## Exercise 1: Configure Agent Locations for the Summary Dashboard

### Scenario

When creating Web Application Availability monitors, you can use the Summary Dashboard to view the health of monitored web applications, including their locations around the globe. You have been asked to display on a map and each agent's location so that operators can instantly view which locations are affected when an issue with a web application is detected.

The main tasks for this exercise are as follows:

1. Create the locations
2. Create location variables
3. Create the agent to location associations

#### ► Task 1: Create the locations

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Manager Shell</b> |
| CMDLet   | <b>New-SCOMLocation</b>         |

2. Type the following commands in the, pressing Enter after each command.

```
New-SCOMLocation -DisplayName "Redmond" -Latitude 47.6739882 -Longitude -122.121512
New-SCOMLocation -DisplayName "Chicago" -Latitude 41.850033 -Longitude -87.6500523
```

#### ► Task 2: Create location variables

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Manager Shell</b> |
| CMDLet   | <b>Get-SCOMLocation</b>         |

2. Type the following commands pressing Enter after each command.

```
$redmond = Get-SCOMLocation -DisplayName "Redmond"
```

3. \$chicago = Get-SCOMLocation -DisplayName "Chicago"

► **Task 3: Create the agent to location associations**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Manager Shell</b> |
| CMDLet   | <b>Get-SCOMLocation</b>         |

2. Type the following commands in the following table, pressing Enter after each command.

```
$Agent = Get-SCOMAgent -Name "LON-SQ1.contoso.com"
set-SCOMLocation -Location $Redmond -Agent $Agent
$Agent = Get-SCOMAgent -Name "LON-DC1.contoso.com"
```

3. set-SCOMLocation -Location \$Chicago -Agent \$Agent

**Results:** After this exercise, you should have used the Operations Manager shell to create two new locations for Redmond and Chicago. You should have also associated these locations with the Operations Manager agents running on LON-SQ1 and LON-DC1.

## Exercise 2: Configure Synthetic Transactions

### Scenario

You have been tasked with monitoring Contoso's line-of-business web applications. These applications are accessed by users from around the world. You must include synthetic transaction monitoring for these applications that simulates end-user activity from multiple locations.

The main tasks for this exercise are as follows:

1. Create a Web Application Availability Monitor
2. View the DinnerNow web application availability by using the Summary and Detailed Dashboards
3. Configure remote connections to LON-AP2
4. Create an OLE DB Data Source Monitor
5. Create a TCP Port Check Monitor

#### ► Task 1: Create a Web Application Availability Monitor

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                          |
|----------|------------------------------------------------|
| Computer | <b>LON-MS1</b>                                 |
| Tool     | <b>Operations Console</b>                      |
| Pane     | <b>Authoring\Management Pack Templates</b>     |
| Template | <b>Web Application Availability Monitoring</b> |

2. Use the Add Monitoring Wizard to configure the Web Application Availability Monitoring Management Pack template, using the following settings (all other settings should remain the default settings):
  - Name: **DinnerNow**
  - Management Pack: **DinnerNow**
  - What to Monitor\Name: **DinnerNow Home Page**
  - What to Monitor URL: **http://LON-AP2/DinnerNow**
  - Where to Monitor: **LON-DC1.CONTOSO.COM** and **LON-SQ1.CONTOSO.COM**
  - Use the **Run Test** option to test the URL and view the results
3. In the **Monitoring** pane, in the **Application Monitoring** folder, open the **Test State** view, and wait until the **DinnerNow Web Site Availability** tests appear and are in a healthy state.

#### ► Task 2: View the DinnerNow web application availability by using the Summary and Detailed Dashboards

1. To perform this task, use the computer and tool information shown in the following table.

| Location | Value          |
|----------|----------------|
| Computer | <b>LON-MS1</b> |

| Location | Value                                                                            |
|----------|----------------------------------------------------------------------------------|
| Tool     | <b>Operations Console</b>                                                        |
| Pane     | <b>Monitoring</b>                                                                |
| View     | <b>Application Monitoring\Web Application Availability Monitoring\Test State</b> |

2. Select a test, and then in the **Tasks** pane, use the **Summary Dashboard – Map** task to view the locations and tests being performed.
3. In the **Tasks** pane, use the **Detailed Dashboard – List** task to view performance data collected for each test.

#### ► Task 3: Configure remote connections to LON-AP2

1. To perform this task, use the computer and tool information shown in the following table.

| Location  | Value                                   |
|-----------|-----------------------------------------|
| Computer  | <b>LON-AP2</b>                          |
| Tool      | <b>SQL Server Configuration Manager</b> |
| Pane      | <b>SQL Server Network Configuration</b> |
| Selection | <b>Protocols for SQLEXPRESS</b>         |

2. In SQL Server Configuration Manager on LON-AP2 enable the TCP/IP protocol in the Protocols for SQL Express section.
3. Restart the **SQL Server (SQLEXPRESS)** service.
4. On LON-SC1 open SQL Server Management Studio and connect to **LON-AP2\SQLEXPRESS**
5. Add a new login for **Contoso\svc\_SCOM2012\_MSAA** and add the **sysadmin** Server Role to the **svc\_SCOM2012\_MSAA** login.

#### ► Task 4: Create an OLE DB Data Source Monitor

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                      |
|----------|--------------------------------------------|
| Computer | <b>LON-MS1</b>                             |
| Tool     | <b>Operations Console</b>                  |
| Pane     | <b>Authoring\Management Pack Templates</b> |
| Template | <b>OLE DB Data Source</b>                  |

2. Use the Add Monitoring Wizard to configure the OLE DB Data Source Management Pack template, using the following settings (all other settings should remain as the default settings):
  - Name: **DinnerNow Database Check**

- Management Pack: **DinnerNow**
  - Connection String: Click **Build**
  - Provider: **Microsoft OLE DB Provider for SQL Server**
  - Computer or device name: **LON-AP2\SQLEXPRESS**
  - Database: **DinnerNow**
  - Query to execute: **Select \* from dbo.menu**
  - Watcher Nodes: **LON-MS1**
3. In the **Monitoring** pane, in the **Synthetic Transaction** folder, open the **OLE DB Data Source State** view, and then wait until the **DinnerNow Database Check** monitor is displayed in a healthy state.

#### ► Task 5: Create a TCP Port Check Monitor

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                      |
|----------|--------------------------------------------|
| Computer | <b>LON-MS1</b>                             |
| Tool     | <b>Operations Console</b>                  |
| Pane     | <b>Authoring\Management Pack Templates</b> |
| Template | <b>TCP Port</b>                            |

2. Use the Add Monitoring Wizard to configure the TCP Port Management Pack template, using the following settings (all other settings should remain the default settings):
  - Name: **DinnerNow Web Site Port Check**
  - Management Pack: **DinnerNow**
  - Computer or device name: **LON-AP2**
  - Port: **80**
  - Watcher Nodes: **LON-SQ1** and **LON-MS1**
3. In the **Monitoring** pane, in the **Synthetic Transaction** folder, open the **TCP Port Checks State** view, and then wait until the **DinnerNow Web Site Port Check** monitor is displayed in a healthy state.

**Results:** After this exercise, you should have used the Operations Manager Management Pack templates to create a Web Application Availability Monitor, an OLE DB Data Source Monitor and a TCP Port Check Monitor for the DinnerNow .NET web application.

## Exercise 3: Create a Distributed Application Diagram for Dinner Now

### Scenario

One of Contoso's key line-of-business applications named DinnerNow is distributed across multiple components. To monitor this application effectively, you must create a Distributed Application Diagram for it that includes the various components that constitute the application.

The main tasks for this exercise are as follows:

1. Create the Distributed Application Diagram
2. Add the Windows Server 2008 Operating System component group
3. Add the IIS Server Role component group
4. Add the SQL Server Role component group
5. Add the Web Application Availability component group
6. Add the DinnerNow Database Availability component group
7. Add the TCP Port Check Component Group
8. Create the relationships between component groups
9. View the Distributed Application Diagram

### ► Task 1: Create the Distributed Application Diagram

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Console</b>       |
| Pane     | <b>Authoring</b>                |
| View     | <b>Distributed Applications</b> |

2. Use the **Create a New Distributed Application** task to create a new Distributed Application Diagram with the following settings (leave all other default settings):
  - Name: **DinnerNow**
  - Template: **Line of Business Web Application**
  - Management Pack: **DinnerNow**.
3. From the **Database** pane, add the DinnerNow database to the DinnerNow Web Application Databases component group
4. From the **Web Site** pane, add the default website for LON-AP2 to the **DinnerNow Web Application Web Sites** component group.

► **Task 2: Add the Windows Server 2008 Operating System component group**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                    |
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Add Component** toolbar option to add a new component group with the following settings:

- Name: **Windows Server 2008 Operating System**
- Objects of the following type(s): **Windows Server 2008 Operating System** from **Object\Configuration Item\Logical Entity\Operating System\Windows Operating System\Windows Server Operating System**
- From the **Windows Server 2008 Operating System** pane, add **LON-AP2.contoso.com** to the **Windows Server 2008 Operating System** component group

► **Task 3: Add the IIS Server Role component group**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                    |
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Add Component** toolbar option to add a new component group with the following settings:

- Name: **IIS Server Role**
- Objects of the following type(s): **IIS Server Role** from **Object\Configuration Item\Logical Entity\Computer Role\Windows Computer Role**

3. From the **IIS Server Role** pane, add **LON-AP2.contoso.com** to the **IIS Server Role** component group.

► **Task 4: Add the SQL Server Role component group**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value          |
|----------|----------------|
| Computer | <b>LON-MS1</b> |

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Add Component** toolbar option to add a new component group with the following settings:
  - Name: **SQL Server Role**
  - Objects of the following type(s): **SQL Role** from **Object\Configuration Item\Logical Entity\Computer Role\Windows Computer Role**
3. From the **SQL Role** pane, add **LON-AP2.contoso.com** to the **SQL Server Role** component group.

► **Task 5: Add the Web Application Availability component group**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                    |
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Add Component** toolbar option to add a new component group, using the following settings:
  - Name: **Web Application Availability**
  - Objects of the following type(s): **Web Application Availability Monitoring Test Base** from **Object\Configuration Item\Logical Entity\Perspective**
3. From the **Web Application Availability Monitoring Test Base** pane, add both objects to the **Web Application Availability** component group.

► **Task 6: Add the DinnerNow Database Availability component group**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                    |
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Add Component** toolbar option to add a new **Component Group** with the following settings:
  - Name: **DinnerNow Database Availability**
  - Objects of the following type(s): **OLE DB Check Perspective** from **Object\Configuration Item\Logical Entity\Perspective**
3. From the **OLE DB check Perspective** pane, add **DinnerNow Database Check** to the **DinnerNow Database Availability** component group.

► **Task 7: Add the TCP Port Check Component Group**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                    |
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Add Component** toolbar option to add a new component group, using the following settings:
  - Name: **TCP Port Availability**
  - Objects of the following type(s): **TCP port check Perspective** from **Object\Configuration Item\Logical Entity\Perspective**
3. From the **TCP port check Perspective** pane, add both objects to the **TCP Port Availability** component group.

► **Task 8: Create the relationships between component groups**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                                             |
|----------|-------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                    |
| Tool     | <b>Operations Console</b>                                         |
| Pane     | <b>Authoring</b>                                                  |
| View     | <b>Distributed Applications\DinnerNow Distributed Application</b> |

2. Use the **Create Relationship** toolbar option to create a relationship by dragging from the source component group to the destination component group, as described in the following table.

| Source component group                     | Destination component group |
|--------------------------------------------|-----------------------------|
| <b>DinnerNow Web Application Web Sites</b> | <b>IIS Server Role</b>      |

| Source component group              | Destination component group          |
|-------------------------------------|--------------------------------------|
| IIS Server Role                     | Windows Server 2008 Operating System |
| SQL Server Role                     | Windows Server 2008 Operating System |
| DinnerNow Web Application Databases | SQL Server Role                      |
| Web Application Availability        | DinnerNow Web Application Web Sites  |
| DinnerNow Database Availability     | DinnerNow Web Application Databases  |
| TCP Port Availability               | DinnerNow Web Application Web Sites  |

3. Click **Save**, and then close the DinnerNow Distributed Application Diagram.

#### ► Task 9: View the Distributed Application Diagram

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Console</b>       |
| Pane     | <b>Monitoring</b>               |
| View     | <b>Distributed Applications</b> |

2. Use the **Diagram View** task from the **Tasks** pane to view the DinnerNow Distributed Application Diagram.

#### Results:

After this exercise, you should have created a Distributed Application Diagram for the DinnerNow web application. The Distributed Application Diagram includes the Database, Web Site, Operating System, IIS Server Role, and SQL Server Role components. After completing the Distributed Application Diagram, you use the Diagram View from the Monitoring pane to view the health of the DinnerNow web application.

## Exercise 4: Create a Visio diagram of the distributed application

### Scenario

You have been tasked with creating a Visio Dashboard that contains the components of the DinnerNow .NET application and then linking the components to the monitored objects in Operations Manager. The health state of components in the Visio Dashboard will then be automatically updated as the objects' health changes in Operations Manager.

The main tasks for this exercise are as follows:

1. Configure the Visio add-in
2. Export the DinnerNow Distributed Application Diagram
3. Import the DinnerNow Distributed Application Diagram into Visio
4. Simulate a failure in DinnerNow and view the health state in the Visio diagram

#### ► Task 1: Configure the Visio add-in

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                       |
|----------|-----------------------------|
| Computer | <b>LON-AP2</b>              |
| Tool     | <b>Microsoft Visio 2010</b> |
| Template | <b>Blank Drawing</b>        |
| Tab      | <b>Operations Manager</b>   |

2. On the **Operations Manager** tab, use the **Configure** option to configure the Operations Manager Data Source as follows:
  - Name: **LON-MS1**
  - Address: **http://LON-MS1/OperationsManager**
  - Automatically Refresh Data: **True**

#### ► Task 2: Export the DinnerNow Distributed Application Diagram

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                           |
|----------|---------------------------------|
| Computer | <b>LON-MS1</b>                  |
| Tool     | <b>Operations Console</b>       |
| Pane     | <b>Monitoring</b>               |
| View     | <b>Distributed Applications</b> |

2. Open the DinnerNow Distributed Application Diagram, and then use the **Export Page to Visio** button to export the page to **\\\lon-ap2\c\$**.
3. Save the diagram as **DinnerNow.vdx**.

► **Task 3: Import the DinnerNow Distributed Application Diagram into Visio**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                       |
|----------|-----------------------------|
| Computer | <b>LON-AP2</b>              |
| Tool     | <b>Microsoft Visio 2010</b> |
| Diagram  | <b>DinnerNow</b>            |
| Location | <b>C</b>                    |

2. Open the **DinnerNow** diagram, and then confirm the Distributed Application Diagram is imported and shows the current health state.
3. In the **Data Source** settings, confirm the **Automatically refresh data** option is selected, and then leave the Visio diagram open.

► **Task 4: Simulate a failure in DinnerNow and view the health state in the Visio diagram**

1. To perform this task, use the computer and tool information in the following table.

| Location | Value                                    |
|----------|------------------------------------------|
| Computer | <b>LON-AP2</b>                           |
| Tool     | <b>Services</b>                          |
| Service  | <b>World Wide Web Publishing Service</b> |
| Action   | <b>Stop</b>                              |

2. On LON-MS1, in the DinnerNow Distributed Application Diagram, wait for the **DinnerNow Web Application** to change to an unhealthy state.
3. On LON-AP2, use the refresh option on the **Operations Manager** tab, and then confirm the **DinnerNow Web Application** changes to an unhealthy state.
4. On LON-AP2, start the **World Wide Web Publishing Service**.
5. In the Distributed Application Diagram, wait for the **DinnerNow Web Application** to return to a healthy state.
6. On LON-AP2, refresh the diagram, and confirm the **DinnerNow Web Application** returns to a healthy state.

**Results:** After this exercise, you should have created a Visio diagram of the DinnerNow Distributed Application Diagram and confirmed that the health state is updated correctly in Visio.

**Question:** When you configure the Web Application Availability Monitoring Management Pack template, you have to monitor the web application from a location that is not included in the Where To Monitor From page of the Add Monitoring Wizard. What must you do?

## Module Review and Takeaways



**Best Practice:** Before you create a Distributed Application Diagram, ensure you have all the relevant information relating to the application or service being monitored. It is recommended that you create an on-boarding document that will help you gather information about the application and ensure all components of the application are discovered, monitored, and included in the Distributed Application Diagram.

### Common Issues and Troubleshooting Tips

| Common Issue                                                                                                    | Troubleshooting Tip |
|-----------------------------------------------------------------------------------------------------------------|---------------------|
| You have created a Distributed Application Diagram, but the Configure Health Roll-Up options are not available. |                     |

### Review Question(s)

**Question:** You need to monitor a Windows Service and generate an alert if the CPU usage rises above 90 percent for more than 15 minutes. When configuring the Windows Service Management Pack template, how should you configure the Performance Data page of the Add Monitoring Wizard?

### Real-world Issues and Scenarios

By default, Distributed Application Diagrams do not generate alerts in Operations Manager. You can change this, however, by performing the following steps:

1. In the Operations console, open the Diagram View.
2. Open the Health Explorer for the root node in the Diagram View.
3. Right-click the root monitor, and then click **Monitor Properties**.
4. On the **Overrides** tab, create an override targeted at the **all objects of class** option.
5. In the **Overrides Properties** window, select the **Override** check box for **Generate Alert**, and then change the **Override Value** to **True**.

# Module 7

## Scorecards, Dashboards, and Reporting

### Contents:

|                                                                           |      |
|---------------------------------------------------------------------------|------|
| Module Overview                                                           | 7-1  |
| <b>Lesson 1:</b> Configuring and Managing Reporting in Operations Manager | 7-3  |
| <b>Lesson 2:</b> Configuring Service Level Tracking                       | 7-10 |
| <b>Lesson 3:</b> Configuring the Operations Manager SharePoint Web Part   | 7-13 |
| <b>Lesson 4:</b> Dashboards and Widgets                                   | 7-16 |
| <b>Lesson 5:</b> Creating Custom Dashboards                               | 7-23 |
| <b>Lab:</b> Configuring Reporting, Dashboards, and Service Level Tracking | 7-27 |
| Module Review and Takeaways                                               | 7-47 |

## Module Overview

One of the key features Operations Manager provides is the ability to quickly and easily create views that reveal service and application health. These views (or dashboards) can instantly display performance and availability for one or more applications in a single pane.

It is important to understand how to create scorecards and dashboards so that you can provide different types of users within the business a view of how the monitored environment is performing. For example, a service owner might require a high-level view showing whether end users are able to access a service, whereas an executive might require only a view showing whether a service is complying with a service level agreement (SLA).

Reporting is an important tool for understanding how the monitored environment is performing. Although certain personnel might not have access to the Operations console or receive alerts by email, they still might need to know important information about the health and performance of key applications and services. In this scenario, reports can be used to provide information about collected Operations Manager data.

Service and application owners must know whether services supplied to the business are meeting SLAs for performance and availability. Therefore, you must know how service level tracking is configured and displayed in Operations Manager.

### Objectives

After completing this module, students will be able to:

- Configure and manage reporting in Operations Manager.
- Configure service level tracking.
- Configure the Operations Manager SharePoint web part.
- Configure dashboards and widgets.
- Create custom dashboards.



## Lesson 1

# Configuring and Managing Reporting in Operations Manager

Operations Manager provides a number of built-in reports that can be run from within the Reporting pane of the Operations console and by using the context-sensitive Report Tasks in the Monitoring pane. As Management Packs are imported into Operations Manager new reports will become available. For example after the Microsoft SQL Server Management Pack is imported a number of SQL Server monitoring reports become available such as the SQL Database Space report. Not all Management Packs include reports however and you must have at least Report Operator privileges in Operations Manager in order to view reports.

Reports provide valuable information for both Operations Console users and non-Operations Console users in the organization that have a requirement to see how the IT environment is performing.

With this in mind it is important that you understand how reports are configured in Operations Manager. This includes how reports can be exported and scheduled so that they can be shared with other people in the organization who do not necessarily have access to the Operations Console.

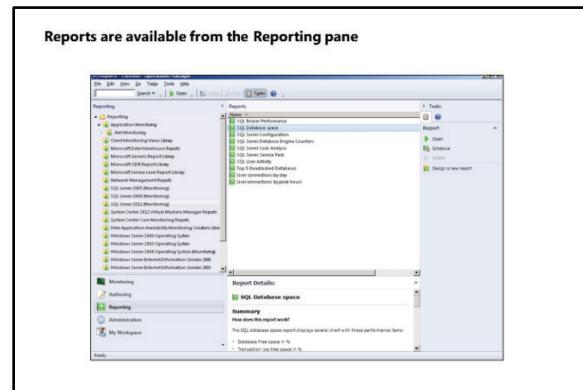
## Lesson Objectives

After completing this lesson, students will be able to:

- Describe Operations Manager reporting.
- Run reports.
- Schedule reports.
- Design reports.

## Operations Manager Reporting Overview

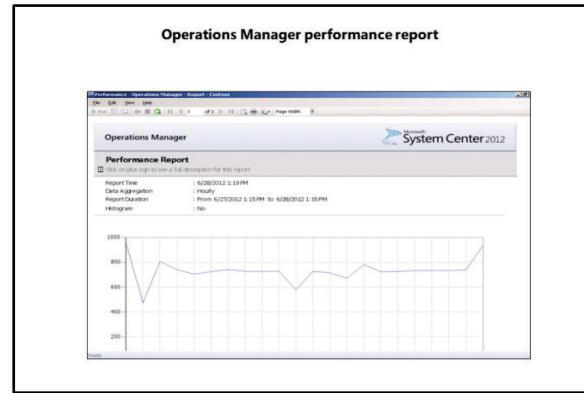
Reporting in Operations Manager is provided by Microsoft SQL Server and SQL Server Reporting Services (SSRS). The reporting components in Operations Manager are described in the following table.



| Reporting component   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Databases             | Both the OperationsManager and OperationsManagerDW databases are used in Operations Manager reports. The OperationsManager database contains the configuration of the Operations Manager Management Group. This includes the Management Packs that are deployed, and the event, performance, and alert data that are collected by agents on monitored computers. The OperationsManagerDW database contains the aggregated data sets that are processed in preparation for reports.                |
| Data Warehouse Server | The OperationsManagerDW database is hosted on the Data Warehouse Server.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Management Server     | Management Servers are responsible for inserting data, such as performance and event data, into the OperationsManager and OperationsManagerDW databases. This insertion is performed by using write actions included in the Management Packs. Also, data is synchronized as an internal job from the OperationsManager database to the OperationsManagerDW database. In most cases, performance data is written to both the OperationsManager and OperationsManagerDW databases at the same time. |
| Reporting Server      | By using SSRS and Microsoft Internet Information Services (IIS), the Operations Manager Reporting Server builds and presents reports. The ReportServer and ReportServerTempDB databases store report definitions that are used for reports in Operations Manager, including any custom reports that are created.                                                                                                                                                                                  |
| Management Packs      | Management Packs contain predefined reports that collect relevant data for the objects that the Management Pack monitors. The slide shows several reports that are included with the SQL Server 2012 Management Pack.                                                                                                                                                                                                                                                                             |

## The Process of Running Reports

Reports can be viewed from the Reporting pane in the Operations console. The number of reports available will grow as Management Packs are imported into Operations Manager. Typically, Management Packs that provide reports create a report folder in the server that is running SSRS, which is displayed in the Reporting pane of the Operations console. For example, after importing the Windows Server 2012 Management Pack, the Windows Server 2012 Operating System (Monitoring) report folder becomes available in the Reporting pane.



Available reports are listed in the details pane. By clicking a report, you display additional information that describes how the report is used. The following table describes information provided in the details pane that is included for each report.

| Report details information   | Description                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| How Does This Report Work?   | A description of the report is provided in this section. Depending on the report type, performance counters, events, and alert types can be displayed. It is important to view this section because it will usually include a list of objects that should be added to the report when you run it. Without reviewing this information, you might include incorrect objects that will cause the report to be rendered without any data. |
| How To Use This Report?      | This section provides information about how to run the report from either the Reporting pane or the Monitoring pane. This section frequently includes information about the objects that should be included in the report.                                                                                                                                                                                                            |
| What Parameters Are Offered? | This section provides details on the parameters that are used in the report to filter the data returned, such as Date/Time and Business hours.                                                                                                                                                                                                                                                                                        |
| Configuration                | Detailed here are typical prerequisites that must be completed for the report to run successfully. For example, in the Disk Performance Analysis report, prerequisite details state that the Discover Windows Logical Disks discovery must be enabled.                                                                                                                                                                                |

 **Note:** It is important to review the Report Details information that is listed in the previous table before you run a report. Report details contain important information about how the report should be configured.

To run reports from the Monitoring pane, the list of available reports is displayed in the Tasks pane under Report Tasks. Running reports from the Monitoring pane is context-sensitive. Depending on what is selected in the Monitoring pane, the list of reports available changes. For example, when you select a computer in the Windows Computers view, several performance reports are available. When you select an alert in the Active Alerts view, reports that relate to alerts are made available.

To run a report from the Monitoring pane, select an object such as a computer from the Windows Computers view, and then in the Tasks pane, click the relevant Report.

To run a report from the Reporting pane, in the report folder, select the report, and then in the Tasks pane, click Open.

For any method that is used to run the report, a new report window is opened. Here, you configure the criteria that should be used to filter the report. Typically, this involves adding objects or groups, setting the From and To dates and times, and selecting the necessary check boxes that relate to the selected report. When you run the report from the Monitoring pane, usually you will find that the objects are automatically populated.

As soon as the report is configured, click the Run button to run the report.

Frequently, links in the report can be useful for running related reports. For example, when the Alert Report is run, a link to the Alert Detail Report is available. Additionally, links to views can be embedded in reports. For example, in the Alert Report just mentioned, a link to the Alert view in the Operations console is displayed. Many generic reports in Operations Manager are used in this way and include links to other reports with predefined values.

## The Process of Scheduling Reports

Scheduling reports provide up-to-date views of the monitored environment, which can be helpful for various reasons. For example, a manager or Chief Information Officer (CIO) might request a daily report of the resource usage for several servers in the environment to justify the expenditure of upgrading systems.

By creating a scheduled report in Operations Manager, you can have the report automatically generated and exported to a document that is stored on a file share. If the SSRS email settings are configured correctly, an additional option to email the reports also becomes available. Reports can then be made available to necessary personnel regularly.

To schedule reports, select a report in the Reporting pane, and then click the Schedule option in the Tasks pane, which starts the Subscribe To A Report wizard. The following table provides details for the related pages in the wizard, including a description of the settings that can be configured.

### **When scheduling reports, you:**

- Specify the report path and type
- Specify the report schedule
- Configure the report criteria
- Can view reports that have been exported in different formats

| Subscribe To A Report page | Options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delivery                   | <p>On the delivery page, you add a name for the Report Schedule. You also configure the delivery method. Delivery method options include the following:</p> <ul style="list-style-type: none"> <li>• <b>Windows File Share.</b> The report is exported and saved to a share.</li> <li>• <b>Null Delivery Provider.</b> The report can be sent to the SSRS cache. This is especially useful if the report takes a long time to generate because of the large amount of data to be processed. Scheduling a report by using the null delivery provider enables the report to be run and cached in SSRS so that it is ready when needed.</li> <li>• <b>E-Mail.</b> The report is generated and then sent to selected people through email by using the To, Cc, Bcc, and Reply addresses. The report format can be configured, including the email priority, the subject line (by default, this is populated with the report name)</li> </ul> |

| Subscribe To A Report page | Options                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <p>and execution time), and a comment field. The email option is made available only when SSRS is configured for email delivery of reports.</p> <p>If the Windows File Share option is selected, you specify the File Name, Path, Render Format such as Excel or Word, the Write Mode such as overwrite or autoincrement, and the credential that is required to run the report.</p>                                                                             |
| Schedule                   | <p>On the Schedule page, you configure when the report should be run. This can include running it only one time, or running it on a schedule: hourly, daily, weekly, or monthly. You can also include a start date and end date for the schedule. For example, you can create a weekly schedule where the report is run on Monday, Wednesday, and Friday, every two weeks, starting on Thursday October 18 at 5:50 A.M. and expiring on Monday, December 24.</p> |
| Parameters                 | <p>On the Parameters page, you can configure or change the report parameters, including adding or removing groups and objects or changing the data aggregation. You can also change the report From and To dates, which is useful when scheduling reports. For example, you can specify date elements such as Previous Week or This Quarter.</p>                                                                                                                 |

As soon as the report is scheduled, it can be viewed in the Scheduled Reports folder in the Reporting pane of the Operations console. With the report selected, you can use the Open task to run the report and the Edit Schedule task to edit the schedule details.

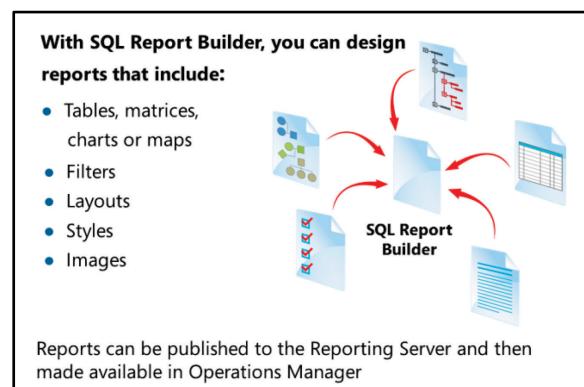
## The Process of Designing Reports

In Operations Manager 2012, reports can be designed with the Microsoft SQL Server Reporting Services Report Builder included with SSRS.

However, before you can use the Report Builder, Report Builder models have to be published to the Report Server.

There are two Report Builder models available on the Operations Manager media. They are located in the ReportModels\Other folder and are named Event.smdl and Performance.smdl. To publish the Report Builder models, you use Microsoft Internet Explorer to browse to the SQL Server Reporting Services Home page. Click the Upload File button to upload the report models. Remember that as soon as the model is uploaded, its data source must be configured. To do this, click the model name on the Home page, and then click the Data Sources tab. Click Browse, select the Data Source, such as Data Warehouse Main, click OK, and then click Apply. The model is now ready to be used in Report Builder.

After the report builder models are published to the reporting server, the Report Builder can be used to create a new report. To open the Report Builder wizard you click the Report Builder button that is available in the home page of the SQL Server Reporting Services website. This is typically [http://<SSRS\\_Server>/Reports](http://<SSRS_Server>/Reports)



### Building a Report by Using the Report Builder Wizard

After the report builder models are published to the reporting server, the Report Builder can be used to create a new report. To open the Report Builder wizard you click the Report Builder button that is available in the home page of the SQL Server Reporting Services website. This is typically [http://<SSRS\\_Server>/Reports](http://<SSRS_Server>/Reports)

You can create a new report by using a wizard in the Report Builder. First, select the report type, such as Table, Matrix, Chart, or Map. Then create a dataset by using either the Event or Performance report model previously uploaded.

### **Adding Fields to Reports**

You can add and filter the data that should be included in the report. You do this by using the Entities and Fields components that are available on the Design A Query page of the wizard.

As an example, suppose that you have to create a report that displays all systems where the Event Log service is stopped within the last 24 hours. In this scenario, from the Entities and Fields section, you drag the related fields to the report. Typical fields would include the following:

- Event Logging Computer Name
- Raw Description
- Event Log Title
- Event Display Number
- Date Time

### **Using the Filter Options**

Using the Filter option on the toolbar, you can filter the data that should be included in the report. In this example scenario described earlier, you drag the following fields to the filter window, and configure them as follows:

- Event Log: System
- Event Display Number: 6006
- Date Time: Within The Last 1 Day

### **Viewing the Report**

To view the report before you publish it so that you can test the filters and make any necessary modifications, you can run the report directly in Report Builder. To do so, on the toolbar, click the exclamation mark button.

### **Arranging the Fields**

You can arrange the fields so that they are displayed correctly in the report. In the example described earlier, you drag the Event\_Logging\_Computer\_Name field to the Row group's box, and drag the Date\_Time field to the Values box.

### **Choosing a Layout**

You can configure the report layout to include subtotals and grand totals. You can also specify whether groups can be expanded or collapsed. In the example described earlier, the default settings are used.

### **Choosing a Style**

When the Report Builder wizard finishes building the report, the report is opened in the Designer, where you can apply a report style such as Ocean or Mahogany to enhance the report's appearance. You can also design the report to include other data sources, datasets, and images.

### **Saving the Report**

You can save the report to the SSRS Server, at which point the report becomes available in the Operations Manager Reporting pane. As soon as the report is published, you can use it in the same way you can use any other report, including scheduling the report and exporting it to a file share.

## Demonstration: Running Reports in the Operations Console

In this demonstration, you will learn how to run a report in Operations Manager.

### Demonstration Steps

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                          |
|----------|------------------------------------------------|
| Computer | <b>LON-MS1</b>                                 |
| Tool     | <b>Operations Console</b>                      |
| Pane     | <b>Reporting</b>                               |
| View     | <b>Windows Server Operating System Reports</b> |

2. Open the **Performance By System** report.
3. Add the **All Windows Computers** group.
4. Change the **From** field from **Today** to **Yesterday**.
5. Run and review the report.
6. Close the report.

**Question:** You have run a report from the Reporting pane in the Operations console.

Unfortunately, no data is shown in the report. What can you do to make sure that important data is included in the report?

## Lesson 2

# Configuring Service Level Tracking

Many organizations set goals for performance and availability of their applications and services to ensure those applications and services are performing at acceptable levels. In Operations Manager, you can use service level objectives to monitor service goals and provide detailed reports and dashboards regarding performance and availability.

To provide these reports and dashboards to the business, you need to understand how service level objectives are configured in Operations Manager. You also need to understand how to use the configured service level objectives in reports.

### Lesson Objectives

After completing this lesson, students will be able to:

- Configure service level objectives.
- Run the Service Level Tracking Summary report.

### The Process of Configuring Service Level Tracking

You can use service level tracking in Operations Manager to monitor and report on service levels for applications and systems. Service level tracking measures the performance of each service level and the service level's availability against predefined goals.

In most cases, you are already collecting the important data that you will use to provide service level tracking reports. Operations Manager provides a method of collating this data into meaningful reports and dashboards that can be used by the business. The slide shows a Service Level Tracking report for IIS website availability. This report shows that a service level objective of 99.00 percent is set against the availability of the IIS website that is running on computer OM1.

The report instantly shows that the service level objectives for this Service Level Tracking monitor are being met.

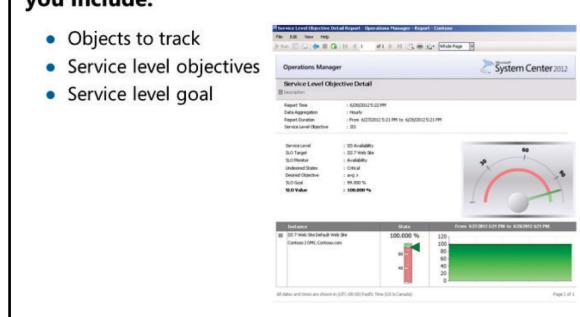
#### Service Level Tracking Wizard

Service level tracking in Operations Manager is configured from the Authoring pane under Management Pack Objects. When you create a Service Level Tracking monitor, you use the Service Level Tracking wizard. When you use the wizard, you must determine the objects that you want to track. You do this by specifying a targeted class. You can specify an already-configured distributed application, a group, or any object that is discovered by Operations Manager. Selecting a distributed application is useful because it includes all application components. You can also scope the objects that you want to track. For example, if you want to monitor the availability of a database, you would set the targeted class to Database, use the scope feature, and then select the relevant database in the tracked target.

Consider the following example. Suppose that you are asked to create a report that shows the availability of a business-critical database named DinnerNow. The report should show when the availability of the database is less than 99.99 percent over a 24-hour period. In this case, you will create a new Service Level

**When you create a Service Level Tracking monitor, you include:**

- Objects to track
- Service level objectives
- Service level goal



Tracking monitor. The following sections describe how the Service Level Tracking Wizard is configured for this report.

### Objects to Track

On the Objects To Track page of the wizard, you set the Targeted class to Database, and then specify a scope that contains the DinnerNow database.

### Specifying Service Level Objective Goals

On the Service Level Objectives page of the wizard, you add a Monitor SLO so that you can track the availability of the object, which in this example is the availability of the DinnerNow database. The resulting report should show that the service level objective is breached if the DinnerNow database is not available for 99.99 percent of the time over a single 24-hour period. You can also add a Collection rule SLO to determine the performance of the database.

You can specify the states that you want to be counted as downtime in the service level objective, such as an unmonitored state or unplanned maintenance state. Finally, you specify the service level objective goal. This is the value with which availability should be measured.

For more information about monitoring Service Level Objectives in Operations Manager visit the following website.

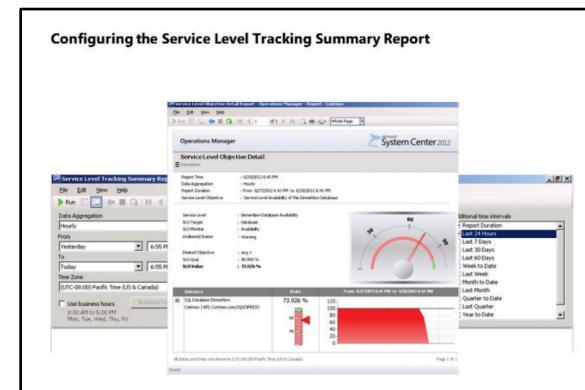
### Monitoring Service Level Objectives by Using Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=404090>

## Service Level Tracking Summary Report

Typically, after the Service Level Tracking monitor is created, the data for the report is available almost immediately. In the Operations Manager Reporting pane, the Microsoft Service Level Report Library folder contains the Service Level Tracking Summary Report.

After you open the report, you add the service levels that you want to include in the report, and specify the report duration. The slide shows that the DinnerNow Database Availability service level is added. The slide also shows that from the Additional time intervals section, the Last 24 Hours option is selected. Additionally, the From field has changed from Today to Yesterday.



When the report is generated, immediately you can determine whether the service level objective goal is being met. The slide shows that over a 24-hour period, the service level objective value is 73.926 percent, and the service level objective goal is 99.990 percent. This reveals that the DinnerNow database has not met the service level objective goal.

You can expand the Service Level section to display the Performance and Availability service level objectives. When you click the hyperlink, the Service Level Objective Detail report is generated. This report displays the Instance, State, and Dates from which the data in the report is generated.

As with all other reports, the Service Level Tracking Summary report can be exported to a different file format such as PDF or Microsoft Word. It can also be scheduled to run on a timed basis and can be published, which makes it available from the Reporting pane.



**Note:** You can also use service level objectives with dashboard views, and you can publish the service level objectives to a Microsoft SharePoint site. This is discussed later in this module.

**Question:** You must configure a Service Level Tracking monitor for a line-of-business web application. You have to make sure that any unplanned maintenance of the website is included when the Service Level Tracking monitor calculates its service level goals. What should you do?

## Lesson 3

# Configuring the Operations Manager SharePoint Web Part

Users of the Operations console (depending on the Operations Manager User Role the users are a member of) can access the Operations console and Web console to view the performance and availability of a monitored environment. You can still provide people who do not have access to the console because of their role within the organization access to certain views or dashboards that have been configured in Operations Manager. You do so by publishing these views and dashboards, via the Operations Manager SharePoint Web Part, to a SharePoint Portal.

Publishing views and dashboards can particularly useful, for example, for service and application owners who do not need to use the Operations console but who do need to know whether service levels are being met within the organization. Using the Operations Manager SharePoint Web Part, a page can be configured in a SharePoint Portal to display a service level dashboard created in the Operations console. Service and application owners can then open the page by using their web browser and quickly determine how service levels are performing.

To provide this functionality in the organization, you need to understand how the Operations Manager SharePoint Web Part is configured.

## Lesson Objectives

After completing this lesson, students will be able to:

- Install the Operations Manager SharePoint Web Part.
- Configure the Operations Manager SharePoint Web Part.

## The Process of Installing the Operations Manager SharePoint Web Part

Integration between Operations Manager and SharePoint is provided by using the Operations Manager SharePoint Web Part. The web part that includes the Windows PowerShell installation script is available from the Operations Manager media in the \Setup\AMD64\SharePoint folder.

### Installing the Operations Manager SharePoint Web Part

To install the web part, you copy the install-OperationsManager-DashboardViewer.ps1 and Microsoft.EnterpriseManagement.SharePointIntegration.wsp Windows PowerShell script files from the Operations Manager media to a location on the SharePoint server.

From the SharePoint 2010 Management Shell, you change the directory to the location where the files were copied, and run the following Windows PowerShell command.

```
.\install-OperationsManager-DashboardViewer.ps1 <location of copied files>
```

**Installing the Web Part involves:**

- Copying files from the Operations Manager media
- Running the Windows PowerShell script

```
Administrator: SharePoint 2010 Management Shell
PS C:\Users\Administrator.CONTOSO> cd\>
PS C:\> .\install-OperationsManager-DashboardViewer.ps1 c: http://localhost:8973
Microsoft System Center Operations Manager 2012 - SharePoint Integration Solution
Deployment Script v1.0
Running Microsoft.SharePoint.PowerShell is loaded
Install-Deploy...
Portal Site is at: http://localhost:8973
Scanning for previous installation remnants...please wait
SUCCESS: No remnant files found.

Going to Add new version of Microsoft.EnterpriseManagement.SharePointIntegration.wsp
Name SolutionId Deployed
microsoft.enterprisemanag... c125f6b7-8c1e-48ae-86e2-bd2d5e568ca2 False
```

During the installation of the web part, you are prompted to select the SharePoint sites to which the web part should be made available. The default is all sites. Or, you can type the SharePoint Portal site URL, which you might want to do if you must restrict web part use to a single SharePoint site.

After the web part is installed, it must be activated. Do this by using the SharePoint 2010 Central Administration site. On the Site Settings page, select the site collection features that are located in the Site Collection Administration section. This section displays the list of features that are available in SharePoint. The Operations Manager Dashboard Web Part is also listed. Click the Activate button next to the web part. This refreshes the Features page. The Activate button changes to a Deactivate button that indicates that the web part is active. In addition, an Active tag is positioned next to the Deactivate button.

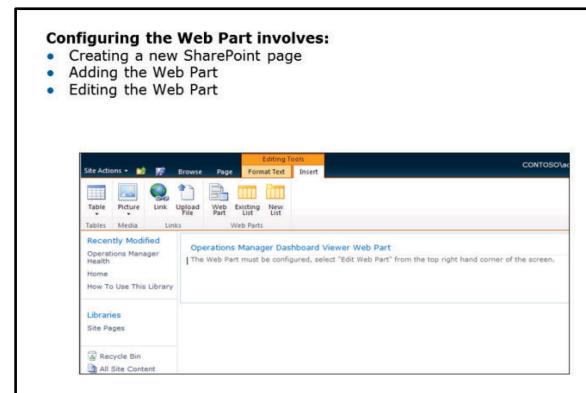
More information about how to use SharePoint to view Operations Manager data can be found at the following webpage:

### Using SharePoint to View Operations Manager Data

<http://go.microsoft.com/fwlink/?LinkId=321877>

## The Process of Configuring the Operations Manager SharePoint Web Part

After the web part is activated, you can configure it to connect to the Operations Manager Web console. To do this, from Site Actions in the Central Administration portal, select View All Site Content. The Operations Manager Web Console Environments item becomes available. Select Operations Manager Web Console Environments, and then click the Add New Item link to create a new item. Configure the new item by using a title, such as **Operations Manager Health**, and a HostURI. The *HostURI* is the URL to the Operations Manager Web console, such as `HTTP://LON-MS1/OperationsManager`.



You can configure other settings, such as the HostErrorTimeout setting. Use this setting to specify a timeout in milliseconds that you should apply when you load the dashboard plug-in. The default setting is 15,000 milliseconds. You can increase this setting in under-performing environments. Save the new item to make it available for a new SharePoint page.

### Creating a New SharePoint Page

To create a new SharePoint page, from the SharePoint sites home page, select Site Actions, and then select the New Page option. Use the new page to display an Operations Manager dashboard view. When you create a new page, you are prompted for a page name. Use a name that does not include spaces, because this name is part of the URL for the page.

After the page is created, use the Insert option to insert the Operations Manager Dashboard Viewer Web Part. Edit the web part to configure the following two elements:

- **Operations Manager web console environments.** Select the newly created item that points to the Operations Manager Web console URL.
- **Dashboard link.** Paste the URL of the Operations Manager dashboard here. Obtain this by starting Internet Explorer, browsing to the Operations Manager Web console, and then selecting the required dashboard view. From the address bar, copy the URL for the dashboard, and then paste it into the Dashboard link.

After you paste the URL of the Operations Manager Web Console Dashboard view into the Dashboard link, save the Operations Manager Dashboard Viewer Web Part properties by clicking OK. Save the new page by clicking Save and Close on the toolbar.

At this point, the SharePoint page is ready to use. You can copy the page URL and email it as a link to relevant staff so that they can view the new page. In addition, a link will be available in the Site Pages view of the SharePoint sites home page.

**Question:** What Operations Manager feature must be installed to use the Operations Manager SharePoint Web Part?

## Lesson 4

# Dashboards and Widgets

When creating dashboard views in Operations Manager, you should understand the various elements that a dashboard view consists of, including the template used to group and display the data, and the widgets used to display the type of data, such as Alerts, State, or Performance. You also need to understand who the audience for your dashboard is so that you can make sure the data you display is both relevant and purposeful.

For example, suppose your IT Manager asks you to create a dashboard view that displays the health state of the computers running SQL Server that host a critical line-of-business application. You would need to create a dashboard view that contained a graph showing the memory, CPU, and disk utilization, and any active critical alerts affecting the servers.

To create this dashboard you need to understand how to use the New Dashboard and Widget Wizard.

### Lesson Objectives

After completing this lesson, students will be able to:

- Describe dashboard view templates.
- Describe dashboard view widgets.
- Use the New Dashboard And Widget Wizard.

### Dashboard View Templates

In Operations Manager, dashboard view templates provide a method of grouping data, which is then displayed in a dashboard, known as the *layout*.

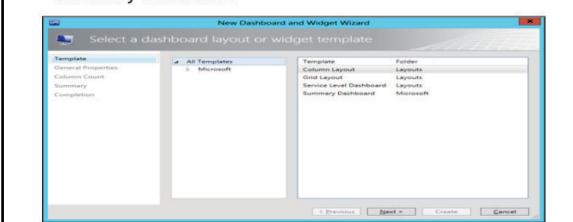
Four layout dashboard templates and an additional layout option control how the data is displayed. These templates and layout options are described in the sections that follow.

#### Column Layout

The Column Layout template uses a dashboard that can include up to five columns. You can use this template to display alert data or health state data. The Column Layout template can also be nested. For example, you can create a view that contains three columns, and one column could include two columns inside it. You can use this template to display many data elements. Instead of having to use multiple views, you can create multiple columns within the same view.

#### Dashboard View Templates include the following:

- Column Layout
- Grid Layout
- Service Level Dashboard
- Summary Dashboard



#### Grid Layout

The Grid Layout template uses a dashboard that can be divided into nine cells. You can use this template when you want to display multiple performance charts. A separate cell can be used for each performance counter, such as Memory, CPU, and Disk. When you select how many cells to include in the dashboard, you also select a layout template. You can use this layout to display different types of data in different views. For example, you can create a 2-Cell layout that displays critical alerts in the top cell and the alert details of a selected alert in the bottom cell.

#### Service Level Dashboard

The Service Level Dashboard template is configured specifically to display service level objectives created in Operations Manager. When you create a dashboard view that uses this template, you select the service level objective that you want to include. Then you select the timeframe in which the data should be displayed, such as the last 24 hours. No other configuration is required when you use this template. As soon you create a dashboard view by using this template, the view displays the overall health state of the service levels, the overall health state of the service level objectives, and a graph and dial that shows the service level goal. You can use this information to immediately determine whether the service levels are being met.

### **Summary Dashboard**

The Summary Dashboard template uses the preconfigured layout of widgets. You can configure these widgets to display the data that meets certain criteria. Included is a Performance Data view, a Performance Chart view, a Health State view, and an Alert view. You can also use this template to display summary information and also performance and availability information for an application or service.

In a nested layout in a dashboard, one element is nested inside another. For example, a grid layout can be nested inside a column layout. Likewise, a column layout can be nested inside a grid layout. A nesting layout is useful because you can present data in different formats within the same dashboard.

More information about how to create views in Operations Manager can be found on the following webpage:

#### **Creating Views in Operations Manager**

<http://go.microsoft.com/fwlink/?LinkId=321898>

## **Dashboard View Widgets**

After the dashboard view is created, you can configure the widgets that display the data in the view. Some of the more common widgets that are used with dashboard views are described in the sections that follow.

### **Alert Widget**

You can use the alert widget to display alerts for a configured scope. The scope can be an object or a group of objects. For example, if you select the All Windows Computers group, the widget will display alerts from all Windows-based computers. You also configure the criteria of alerts that the widget should display. For example, you can select only alerts that have a severity of critical, or alerts that have a high priority. You can use the criteria to combine it with the scope to change the objects that you want to display alerts for, and for the type of alerts that should be displayed. For example, you can display new alerts that have a critical severity state for the IIS Computer Group, configure the widget to display several columns such as the Path, Category, and Owner, and then sort the information by these columns.

**Dashboard view widgets include the following:**

- Alert widget
- Details widget
- Instance details widget
- SLA widget
- Performance widget
- State widget



The screenshot shows the 'Monitoring' workspace in the Operations Manager console. On the left, the navigation pane includes 'Monitoring' (selected), 'Active Alerts', 'Discovery Inventory', 'Distributed Applications', 'IIS', 'Windows Computers', 'Windows Monitoring', 'Application Monitoring', 'Data Minimization', 'Encryption', 'Dimensions Availability', 'Health', 'Microsoft Audit Collection Service', 'Microsoft SQL Server', 'Audit', and 'Process'. The main area displays a list titled 'Critical Alerts (1)'. One alert is listed: 'Default Web Site' with a red warning icon, indicating 'Maintenance Mode' and 'IIS Web Site is unavailable' for 49 minutes. Below the alert list, the 'Alert Details' pane shows the alert's description ('IIS Web Site is unavailable after the site has been stopped'), source ('Default Web Site'), path ('IIS-AP1.LON-CONTORBO.COM'), and status ('Web Site available'). The bottom right of the pane shows a toolbar with icons for 'Edit Properties', 'Delete', 'Set Resolution State', 'Entity Properties', and 'Health Explorer'.

### **Details Widget**

To include details such as alert information you can use the details widget in combination with another widget. For example, combine the details widget with an alert widget so that when an alert is selected, the details widget shows the alert details. If you use the details widget with a state widget, when an object is selected in the state widget, the details widget shows the object's details. You can use the details widget when there are many objects to display, such as Windows-based computers. You can also use the details

widget to display the properties for each computer without creating a view for each computer. The details widget is context-sensitive, so it automatically updates based on what is selected in the associated widget.

### **Instance Details Widget**

You can use the instance details widget to display the details and the state of the configured group or object. When you configure the instance details widget, you select the group or object that the widget should display, such as Windows Computer.

### **SLA Widget**

You can use the SLA widget to display the performance and availability goals and the results of the configured service level objectives. You can use the SLA widget to add multiple service level objectives into one view and to immediately determine whether service level goals are being met.

### **Performance Widget**

You can use the performance widget to display performance counter values in a chart from selected objects or groups. For example, you can scope the performance widget to All Windows Computers, and add the Available Mbytes counter to create a chart that displays the available megabytes of memory on each computer. You could then scope the performance widget with a time range, configuring it to automatically update the data and specify data within the last 24 hours. You can also include several column details, such as Minimum, Maximum, and Average Values.

### **State Widget**

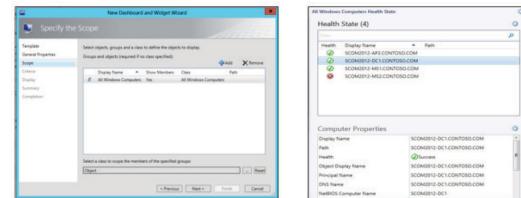
You can use the state widget to display the health state of a class, group, or object. You can use the state widget to view the health state for many objects, or a group in a single view. For example, you can add several unrelated objects and view the health state of each in the same view. When you configure the state widget, you add the related objects or groups that should be included in the view. Then, you select a class to scope the members of the selected group. You can also specify criteria to filter the objects that are displayed.

## The Process of Creating a Dashboard View by Using the New Dashboard and Widget Wizard

To create a dashboard view in Operations Manager, you use the New Dashboard And Widget Wizard. To start the New Dashboard And Widget Wizard, in the Operations console, in the Monitoring pane, right-click a folder, point to New, and then click Dashboard View. The following table describes each page of the New Dashboard And Widget Wizard when a dashboard view is created. Using a grid layout template, the dashboard view is configured to display the health state of all Windows-based computers and contains the state widget and the details widget.

### Use the New Dashboard And Widget Wizard to create dashboard views, including the following:

- Templates to determine layout
- Widgets to determine what data is displayed



| New Dashboard And Widget Wizard page, when creating a dashboard view | Description                                                                                                                            |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Template                                                             | Select the template that will be used to determine the layout of the dashboard. In this example, the Grid Layout template is selected. |
| General Properties                                                   | Specify a name for the dashboard. In this example, the name is All Windows Computers Health State.                                     |
| Layout                                                               | Select the number of cells to display in the dashboard. In this example, 2 Cells is selected, with the cells displayed horizontally.   |
| Summary                                                              | Review the options that are selected. If necessary, go back through the wizard and make any changes.                                   |

As soon as the new dashboard view is created, the widgets can be configured by clicking the Click To Add Widget link. The process of configuring a state widget is described in the following table.

| New Dashboard And Widget Wizard page, when configuring a state widget | Description                                                                                                                                                      |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template                                                              | Configure the widget type. In this example, State Widget is selected.                                                                                            |
| General Properties                                                    | Enter a name that will be displayed as the widget name in the dashboard. In this example, the name will be Health State.                                         |
| Scope                                                                 | Add groups and objects to which the widget will be scoped. In this example, the All Windows Computers group is added.                                            |
| Criteria                                                              | Limit the objects that are displayed by selecting the related health states. In this example, nothing is selected because all health states should be displayed. |
| Display                                                               | Include additional columns to display, such as Path and Display Name. You can also sort and group by these                                                       |

| New Dashboard And Widget Wizard page, when configuring a state widget | Description                                                                                          |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
|                                                                       | columns. In this example, the Health and Display Name columns are selected.                          |
| Summary                                                               | Review the options that are selected. If necessary, go back through the wizard and make any changes. |

After you configure the state widget, you can configure the details widget by clicking the Click To Add Widget link. The following table describes how to configure a details widget.

| New Dashboard And Widget Wizard page, when configuring a details widget | Description                                                                                                      |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Template                                                                | Configure the widget type. In this case, Details Widget is selected.                                             |
| General Properties                                                      | Enter a widget name that will be displayed in the dashboard. In this case, the name will be Computer Properties. |
| Summary                                                                 | Review the options that are selected. If necessary, go back through the wizard and make any changes.             |

After you configure the second widget, the dashboard view is completed. When you click a computer in the Health State view, the Computer Properties view is automatically updated to show the full details of the computer. Additionally, the Windows Computer tasks, such as Computer Management, Ping Computer, and Remote Desktop, can be used in the context of the selected computer. Reports for selected computers can also be opened and run from here, for example, the Health Report that displays the availability of the selected computer.



**Note:** Dashboard views can also be created by using the Operations Manager Web console.

## Demonstration: Creating a Dashboard View

In this demonstration you will learn how to create a Dashboard View by using the Operations Console.

### Demonstration Steps

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>DinnerNow</b>          |

2. Right-click the **DinnerNow** folder, and then create a new dashboard view with the following settings (all the other settings should remain the default settings):

Template: **Column Layout**

Name: **DinnerNow Critical and Warning Alerts**

Column Count: **2**

3. Configure the left widget by using the following settings (all the other settings should remain the default settings):

- Template: **Alert Widget**
- Name: **Critical and Warning Alerts**
- Scope: **Select Groups and Objects**; type **dinnernow** to search, and then select **DinnerNow - Production**, where **.NET Application Component Group** is displayed in the **Class** column
- Criteria: **Critical and Warning**

4. Configure the right widget and use the following settings (all the other settings should remain the default settings):

- Template: **Details Widget**

- Name: **Alert Details**

5. In the **DinnerNow Critical and Warning Alerts** dashboard, select an alert in the **Critical and Warning Alerts** column.

6. In the **Alert Details** column, notice that the alert details for the selected alert are displayed.

**Question:** You are asked to create a dashboard view. This dashboard view must include the six performance graphs that show collected performance data relating to the following:

- Memory utilization
- Processor utilization
- Disk utilization
- Network utilization
- Database free space
- Web Transaction Response Time

**Question:** What are the best template and widgets to use in the dashboard view?

## Lesson 5

# Creating Custom Dashboards

Dashboard views are typically created from the Operations console or Web console, however, there is a free tool available that can make this even easier and adds some extra functionality. This tool is the GTM.exe tool available from the System Center: Operations Manager Engineering Blog.

Using this tool, you can use components of Operations Manager dashboards to add the following key capabilities:

- Create custom dashboards that can reside in any Management Pack folder in the Operations Manager monitoring pane
- Export custom dashboards so that they can be used in any other Management Group
- Launch custom dashboards from the task pane when you target a specific computer or object

### Lesson Objectives

After completing this lesson, students will be able to:

- Describe how to create a dashboard view that can be opened from any Management Pack folder or exported to any Management Group.
- Describe how to create a dashboard view that can be run from an Operations Manager task.

### The Process of Creating a Dashboard View in the Microsoft Windows Server Folder

You can use the GTM tool to make published dashboard views available from any folder in the Monitoring pane of the Operations console. You can also use this tool to create a dashboard view from a folder that is stored in a sealed Management Pack, such as the Microsoft Windows Server folder that is stored in the Windows Server Operating System Library Management Pack.

The following table describes the steps for publishing a dashboard view to the Microsoft Windows Server folder. The dashboard view uses a grid layout template that will be used to display performance counter information for selected computers in the view.

**Steps to publish a dashboard in the Microsoft Windows Server folder include the following:**

1. Create a new Management Pack
2. Create a new dashboard view
3. Export the Management Pack
4. Copy the GTMTool utility
5. Run the GTMTool utility
6. Configure the GTMTool prompts
7. Import the Management Pack

| Steps for publishing a dashboard view to Microsoft Windows Server folder | Description                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Create a new Management Pack.                                         | A new Management Pack is created to store the new dashboard view.                                                                                                                                                                                                                                        |
| 2. Create a new dashboard view.                                          | A dashboard view is created in the folder in which the new Management Pack is created. The Grid Layout template is used for the view, and the performance widgets are added to the view that is scoped to the Windows Server Computer Group. Then, you can add the performance counters for objects such |

| Steps for publishing a dashboard view to Microsoft Windows Server folder | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                          | as CPU, Memory, and Disk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 3. Export the Management Pack.                                           | The Management Pack is exported to a local folder on the Management Server, such as C:\Export.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 4. Copy the GTMTool utility.                                             | The GTMTool utility files are also copied to the C:\Export folder on the Management Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 5. Run the GTMTool utility.                                              | <p>The GTMTool utility is run at a command prompt in the C:\Export folder by using the following syntax.</p> <pre data-bbox="703 650 1279 705">GTMTool.exe /SRC &lt;SourceMPFile&gt; /SRV ManagementServerName /OUT &lt;OutputLocation&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 6. Configure the GTMTool messages.                                       | <p>During the processing of the Management Pack, you receive a message from the GTMTool asking whether you also want to create a task for the dashboard. In this case, enter <b>N</b>.</p> <p>The GTM Tool also sends a message that asks for the Management Pack that should be used when it is imported. In this case, enter <b>Microsoft.Windows.Server.Library</b> to indicate the Microsoft Windows Server Management Pack. A list of folders that are available in the Management Pack is displayed. Enter the name of the folder in which the dashboard view should be displayed. In this case, enter <b>Microsoft Windows Server</b>.</p> <p>A new Management Pack is then created and saved in the folder that is specified by using the OUT switch.</p> |
| 7. Import the Management Pack.                                           | The Management Pack is imported into Operations Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

After the Management Packs are imported, you can view the new dashboard view. The new dashboard view is located in the Microsoft Windows Server folder on the Monitoring pane of the Operations console.

More information about how to create custom dashboards can be found on the following webpage:



### System Center: Operations Manager Engineering Blog

<http://go.microsoft.com/fwlink/?LinkId=321899>

## The Process of Creating a Dashboard View that Can Be Run from the Tasks Pane

In the example in the previous topic, a dashboard view is created in the Microsoft Windows Server folder. This view is scoped to the Windows Server Computer Group, so all Windows Servers will be included in the view. You can also use the GTM tool to create a task in the Tasks pane of the Operations console, which opens a dashboard view, and scope the dashboard view to any monitored computer in the Operations Manager environment.

To create a dashboard view (as described in the previous topic) that can be run from the Tasks pane, follow the steps described in the following table.

The steps to create a dashboard are the same as when publishing a dashboard to the Microsoft Windows Servers folder, except you target a monitored computer object instead of a group

| Steps for creating a dashboard view | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Create a new Management Pack.    | A new Management Pack is created to store the new dashboard view.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 2. Create a new dashboard view.     | A dashboard view is created in the folder in which the new Management Pack is created. The Grid Layout template is used for the view, and the performance widgets are added to the view that is scoped to a monitored computer. Performance counters are added for objects, such as CPU, Memory, and Disk. Make sure that the scope is set to a monitored computer object. You achieve this by clicking the Groups And Objects option on the Scope And Counters page of the Select A Group Or Object dialog box in the of the New Dashboard And Widget Wizard. You enter the name of the computer, such as LON-DC1, and then select the object where the Class column displays Windows Computer. |
| 3. Export the Management Pack.      | The Management Pack is then exported to a local folder on the Management Server, such as C:\Export.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 4. Copy the GTMTool utility.        | The GTMTool utility files are also copied to the C:\Export folder on the Management Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 5. Run the GTMTool utility.         | <p>The GTMTool utility is then run at a command prompt in the C:\Export folder by using the following syntax.</p> <pre data-bbox="763 1628 1339 1691">GTMTool.exe /SRC &lt;SourceMPFile&gt; /SRV<br/>ManagementServerName /OUT &lt;OutputLocation&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 6. Configure the GTMTool prompts.   | <p>During the processing of the Management Pack, you receive a message from the GTM tool asking whether you also want to create a task for the dashboard. In this case, enter <b>Y</b>.</p> <p>The GTM tool also sends a message that asks for the Management Pack that should be used when it is imported. In this case, enter <b>Microsoft.Windows.Server.Library</b> to indicate the Microsoft Windows Server Management Pack. A list of folders that are available in the Management Pack is displayed. Enter the folder</p>                                                                                                                                                                 |

| Steps for creating a dashboard view | Description                                                                                                                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | name of the folder in which the dashboard view should be displayed. In this case, enter <b>Microsoft Windows Server</b> . A new Management Pack is then created and saved in the folder that is specified by using the OUT switch. |
| Import the Management Pack.         | The Management Pack is imported into Operations Manager.                                                                                                                                                                           |

After the Management Pack is imported, you can select any computer from the Windows Computers view, in the Monitoring pane of the Operations console. Now the Windows Server Task Pane Dashboard Task becomes available in the Tasks pane under Navigation. When the task is run, the dashboard view is opened and is automatically scoped to the selected computer.

**Question:** What are the two main features for which the GTM tool is used?

# Lab: Configuring Reporting, Dashboards, and Service Level Tracking

## Scenario

Your IT Manager is concerned that a number of servers in the environment (including the server that hosts the DinnerNow database) are restarting unexpectedly and has asked you to investigate further.

The IT Manager has requested a weekly report that shows how often production servers are being restarted. The report should be run on a weekly basis and be automatically saved in MHTML format to a file share that can be accessed over the network. You decide to use the Report Builder to build this report.

**To keep track of the performance and availability of the DinnerNow application, you also decide to create a number of dashboards and configure service level tracking for DinnerNow.**

After completing this lab, students will be able to:

- Design a custom report in Operations Manager.
- Schedule the report.
- Create a Service Level Tracking monitor.
- Configure an Alert Dashboard.
- Configure a Performance Dashboard.
- Configure a Summary Dashboard.
- Configure an SLA Dashboard and publish the dashboard to SharePoint.
- Use the GTM tool to publish a custom dashboard.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machines:** 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-AP1, 10964C-LON-AP2

**User Name:** Contoso\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:
  - 10964C-LON-SQ1
  - 10964C-LON-MS1

- 10964C-LON-AP1
- 10964C-LON-AP2

 **Note:** Before you start this lab, make sure that all Windows Services that are set to start automatically are running. The exceptions are for the Microsoft .NET Framework NGEN v4.0.30319\_X86 and .NET Framework NGEN v4.0.30319\_X64 services, because these services stop automatically when they are not being used.

## Exercise 1: Design a New Report

### Scenario

You know that the Windows operating system logs event 6005 when a server is restarted. You decide to build a custom report that is based on the Event ID. However, before you can design the report, you have to import the Event report model into the Report Server. Then, the Event report model can be used by Report Builder when you design the report.

The main tasks for this exercise are as follows:

1. Import the report model into the Report Server
2. Design a new report using Report Builder
3. View the report

#### ► Task 1: Import the report model into the Report Server

1. To perform this step, use the computer and tool information in the following table.

| Location     | Value                         |
|--------------|-------------------------------|
| Computer     | <b>LON-MS1</b>                |
| Tool         | <b>Internet Explorer</b>      |
| URL          | <b>HTTP://LON-SQ1/Reports</b> |
| Report Model | <b>Event.smdl</b>             |

2. Browse to **HTTP://LON-SQ1/Reports**, and then use the **Upload File** option to upload the **Event.smdl** report model from the **\LON-DC1\Media\SCOM2012R2\ReportModels\Other** folder.
3. After you upload the report model, edit the properties, and then set the Data Source to **Data Warehouse Main**.

#### ► Task 2: Design a new report using Report Builder

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                                                                            |
|----------|----------------------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                                   |
| Tool     | <b>Report Builder</b>                                                            |
| URL      | <b>http://LON-SQ1/reportserver/reportbuilder/reportbuilder_3_0_0.application</b> |

2. Use the **Design A New Report** task to design a report that includes the following settings (all other settings should remain as the default settings):
  - Use the Chart Wizard.
  - Select the **Event** data source.
  - Add the **Event Logging Computer Name** field from the **Event Entity**.
  - Add the **#Events** field from the **Event Entity**.
  - Use the **Filter** option to configure the following:
    - a. Add the **Event Display Number** filter and configure it to filter event ID **6005**.
    - b. Select the Column chart type.
    - c. Add the **Event\_Logging\_Computer\_Name** field to the Categories section.
    - d. Add the **ID\_Events** field to the Values section.
    - e. Rename the Chart Title to Number of computer restarts in the last seven days.
    - f. Rename the x Axis to Computer.
    - g. Rename the y Axis to No. of restarts.
    - h. Delete the **ID Events Legend**.
3. Save the report to **Microsoft.Windows.Server.2012.Monitoring**, and then name the report **Number of computer restarts within the 7 seven days.rdl**.

#### ► Task 3: View the report

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                                                    |
|----------|----------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                           |
| Tool     | <b>Operations Console</b>                                |
| Pane     | <b>Reporting</b>                                         |
| Folder   | <b>Windows Server 2012 Operating System (Monitoring)</b> |

2. Open the **Number Of Computer Restarts Within The Last 7 Days** report.

**Results:** After this exercise, you should have used Report Builder to design a new report that shows how many times in the last seven days the computers have restarted. Also, you should have saved the report to the SSRS so that the report is available from the Reporting pane of the Operations console.

## Exercise 2: Schedule Reports

### Scenario

With the report designed and available in the Reporting pane, you now have to configure a schedule so that the report can be automatically generated weekly. When the report is generated, it should be made available in shared folder that can be accessed over the network and saved in MHTML format.

The main tasks for this exercise are as follows:

1. Create a file share and schedule the report
2. Confirm the report schedule is working as expected

► **Task 1: Create a file share and schedule the report**

1. To perform the next step, use the computer and tool information shown in the following table.

| Location   | Value                   |
|------------|-------------------------|
| Computer   | <b>LON-MS1</b>          |
| Tool       | <b>Windows Explorer</b> |
| File Share | <b>Reports</b>          |

2. Create a folder named **Reports** on drive C of LON-MS1, and share it by using read/write permissions for everyone.
3. To perform the rest of the steps, use the computer and tool information in the following table.

| Location | Value                                                              |
|----------|--------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                     |
| Tool     | <b>Operations Console</b>                                          |
| Pane     | <b>Reporting</b>                                                   |
| View     | <b>Microsoft Windows Server 2012 Operating System (Monitoring)</b> |

4. Open the Number Of Computer Restarts Within The Last 7 Days report, and use the **Schedule** option on the **File** menu to schedule the report with the following settings (all other settings should remain as the default settings):
  - Description: **Number of computer restarts within the last 7 days**
  - Delivery method: **Windows File Share**
  - File name: **Number of computer restarts within the last 7 days.mhtml**
  - Path: **\\\\ LON-MS1\\Reports**
  - Render format: **MHTML**
  - Write mode: **Autoincrement**
  - User name: **Contoso\\Administrator**
  - Password: **Pa\$\$w0rd**
  - Subscription Schedule: **Weekly**
  - Increase the start time by two minutes

► **Task 2: Confirm the report schedule is working as expected**

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value |
|----------|-------|
|          |       |

| Location | Value                                                           |
|----------|-----------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                  |
| Tool     | <b>Windows Explorer</b>                                         |
| Folder   | <b>C:\Reports</b>                                               |
| File     | <b>Number of computer restarts within the last 7 days.mhtml</b> |

2. Refresh the C:\Reports folder until the **Number of computer restarts within the last 7 days.mhtml** report becomes available.
3. Open and review the report.
4. Close the report.

**Results:** After this exercise, you should have scheduled the Number Of Computer Restarts Within The Last 7 Days report to run weekly, and then exported this report as an MHTML file to the Reports share site on LON-MS1. You should also have confirmed that the schedule works as expected and that the report is generated.

## Exercise 3: Configure Service Level Tracking for DinnerNow

### Scenario

For the service owner to view performance and availability metrics for DinnerNow, you decide to create a service level objective monitor that can be used to monitor the service level goals for DinnerNow.

The main tasks for this exercise are as follows:

1. Create a service level objective
2. View the Service Level Tracking Summary Report

#### ► Task 1: Create a service level objective

1. To perform the next step, use the computer and tool information shown in the following table.

| Location | Value                         |
|----------|-------------------------------|
| Computer | <b>LON-MS1</b>                |
| Tool     | <b>Operations Console</b>     |
| Pane     | <b>Authoring</b>              |
| View     | <b>Service Level Tracking</b> |

2. Use the Create task to create a service level objective with the following settings (all other settings should remain the default settings):
  - Name: **DinnerNow**
  - Objects to Track: **IIS 7 Web Server**
  - Scope: **LON-AP2.CONTOSO.COM** where the **Class** column displays **Windows Server 2008 R2 Full Computer**.
  - Management Pack: **DinnerNow**
  - Service Level Objectives: **Monitor State SLO** set to **Availability** with a name of **Availability**

#### ► Task 2: View the Service Level Tracking Summary Report

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                    |
|----------|----------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                           |
| Tool     | <b>Operations Console</b>                                |
| Pane     | <b>Reporting\ Microsoft Service Level Report Library</b> |
| Report   | <b>Service Level Tracking Summary Report</b>             |

2. Open the Service Level Tracking Summary Report, and then add the DinnerNow service level objective.
3. Change the **From** field to **Yesterday**, and then run the report.

4. Expand **LON-AP2.CONTOSO.COM**, and then select **Availability**.

**Results:** After this exercise, you should have configured a Service Level Object that is targeted at the DinnerNow Web Server. You should have also run the Service Level Tracking Summary Report and included the DinnerNow service level tracking objective.

## Exercise 4: Configure an Alert Dashboard

### Scenario

You have to create an Alert Dashboard that displays Critical and Warning alerts for the DinnerNow .Net Framework application. The view should let both the alert and the alert details to be displayed in a single view.

The main tasks for this exercise are as follows:

1. Create the dashboard
2. Configure the widgets
3. Use the Alert Dashboard

#### ► Task 1: Create the dashboard

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>DinnerNow</b>          |

2. Right-click the **DinnerNow** folder, and then create a new dashboard view with the following settings (all the other settings should remain the default settings):
  - Template: **Column Layout**
  - Name: **DinnerNow Critical and Warning Alerts**
  - Column Count: **2**

#### ► Task 2: Configure the widgets

1. To perform this step, use the computer and the tool information shown in the following table.

| Location | Value                                          |
|----------|------------------------------------------------|
| Computer | <b>LON-MS1</b>                                 |
| Tool     | <b>Operations Console</b>                      |
| Pane     | <b>Monitoring\Monitoring\</b> <b>DinnerNow</b> |

| Location | Value                                        |
|----------|----------------------------------------------|
| View     | <b>DinnerNow Critical and Warning Alerts</b> |

2. Configure the left widget by using the following settings (all the other settings should remain the default settings):
  - Template: **Alert Widget**
  - Name: **Critical and Warning Alerts**
  - Scope: **Select Groups and Objects**; type **dinnernow** to search, and then select **DinnerNow - Production**, where **.NET Application Component Group** is displayed in the **Class** column
  - Criteria: **Critical and Warning**
3. Configure the right widget and use the following settings (all the other settings should remain the default settings):
  - Template: **Details Widget**
  - Name: **Alert Details**

### ► Task 3: Use the Alert Dashboard

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                                        |
|----------|----------------------------------------------|
| Computer | <b>LON-MS1</b>                               |
| Tool     | <b>Operations Console</b>                    |
| Pane     | <b>Monitoring\{DinnerNow</b>                 |
| View     | <b>DinnerNow Critical and Warning Alerts</b> |

2. In the **DinnerNow Critical and Warning Alerts** dashboard, select an alert in the **Critical and Warning Alerts** column.
3. In the **Alert Details** column, notice that the alert details for the selected alert are displayed.

**Results:** After this exercise, you should have created a dashboard view that uses the alert and details widgets to display critical and warning alerts for the DinnerNow .NET Framework application.

## Exercise 5: Configure a Performance Dashboard

### Scenario

You have to create a dashboard view that displays specific performance counter information for the DinnerNow .NET Framework application. The view should show the Total Transaction Response time and Total Monitored Requests/Sec for the DinnerNow website. This information will be used to monitor the performance of the website from an end-user perspective.

The main tasks for this exercise are as follows:

1. Create the dashboard
2. Configure the widgets

#### ► Task 1: Create the dashboard

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| Folder   | <b>DinnerNow</b>          |

2. Right-click the **DinnerNow** folder, and create a new **Dashboard View** using the following settings (all the other settings should remain the default settings):

- Template: **Grid Layout**
- Name: **DinnerNow – End User Performance**
- Layout: **2 Cells (second cell type)**

#### ► Task 2: Configure the widgets

1. To perform this step, use the computer and the tool information shown in the following table.

| Location | Value                                          |
|----------|------------------------------------------------|
| Computer | <b>LON-MS1</b>                                 |
| Tool     | <b>Operations Console</b>                      |
| Pane     | <b>Monitoring\Monitoring\</b> <b>DinnerNow</b> |
| View     | <b>DinnerNow – End User Performance</b>        |

2. Configure the first widget, and then use the following settings (all the other settings should remain the default settings):

- Template: **Performance Widget**
- Name: **Average Request Time (Seconds)**

- Scope and Counters: Select **Groups and Objects**; type **dinnernow** to search, and then select **Default Web Site/DinnerNow**, where **ASP.NET Application** is displayed in the **Class** column.
- Add the following performance counter:
  - Object: **.NET Apps**
  - Counter: **Avg. Request Time (seconds)**
  - Available items: Select **NET Apps**, where the **Performance Instance** column does not display **(All)**
- 3. Configure the second widget by using the following settings (all the other settings should remain the default settings):
  - Template: **Performance Widget**
  - Name: **Exception Events (Per Second)**
  - Scope and Counters: Select **Groups and Objects**; type **dinnernow** to search, and then select **Default Web Site/DinnerNow**, where **ASP.NET Application** is displayed in the **Class** column
  - Add the following performance counter:
    - Object: **.NET Apps**
    - Counter: **Exception Events/sec**
    - Available items: Select **NET Apps**, where the **Performance Instance** column does not display **(All)**

**Results:** After this exercise, you should have created a new dashboard view that uses the performance widget. You should have added the Transaction Response Time and Total Monitored Requests/Sec performance counters that the widgets display in the dashboard.

## Exercise 6: Configure a Summary Dashboard

### Scenario

You have to create a Summary Dashboard that can be used to monitor the performance and availability of the DinnerNow database server. The view should include the health state of the database server. The view should also include the performance counters that show the database free space as both a percentage and in megabytes (MB).

The main tasks for this exercise are as follows:

1. Create the dashboard
2. Configure the widgets

#### ► Task 1: Create the dashboard

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| Folder   | <b>DinnerNow</b>          |

2. Right-click the **DinnerNow** folder, and create a new **Dashboard View** by using the following settings (all the other settings should remain the default settings):

- Template: **Summary Dashboard**
- Name: **DinnerNow**

#### ► Task 2: Configure the widgets

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                               |
|----------|-------------------------------------|
| Computer | <b>LON-MS1</b>                      |
| Tool     | <b>Operations Console</b>           |
| Pane     | <b>Monitoring\</b> <b>DinnerNow</b> |
| View     | <b>DinnerNow</b>                    |

2. Configure the **Top N** widget by clicking the configuration icon and then clicking **Configure**. Configure the following settings (all the other settings should remain the default settings):

- 3. Name: **Database Free Space (MB)**
- 4. Scope and Counters: Select **Groups and Objects**; type **dinnernow** to search, and then select **DinnerNow**, where the **Class** column displays **SQL Database**
- 5. Add the following performance counter:
  - Object: **MSSQL\$SQLEXPRESS:Database**

- Counter: **DB Total Free Space (MB)**
  - Instance: **DinnerNow**
  - Available items: **DinnerNow**
6. Configure the **Performance** widget by clicking the configuration icon and then clicking **Configure**. Configure the following settings (all the other settings should remain the default settings):
- Name: **Database Free Space (%)**
  - Scope and Counters: Select **Groups and Objects**; type **dinnernow** to search, and then select **DinnerNow**, where the **Class** column displays **SQL Database**
7. Add the following performance counter:
- Object: **MSSQL\$SQLEXPRESS:Database**
  - Counter: **DB Total Free Space (%)**
  - Instance: **DinnerNow**
  - Available items: **DinnerNow**
8. Configure the **State** widget by clicking the configuration icon and then clicking **Configure**. Configure the following settings (all the other settings should remain the default settings):
- Name: **SQL Server Health State**
  - Scope: Select **Show all Objects and Groups**; type **SQL** to search, and then select **SQLEXPRESS**, where the **Path** column displays **LON-AP2.CONTOSO.COM**
9. Configure the **Alerts** widget by clicking the configuration icon and then clicking **Configure**. Configure the following settings (all the other settings should remain the default settings):
- Name: **All SQL Server Alerts**
  - Scope: Select **Groups and Objects**; type **SQL** to search, and then select **SQLEXPRESS**, where the **Path** column displays **LON-AP2.CONTOSO.COM**



**Note:** If the **MSSQL\$SQLEXPRESS:Database** performance counter is not available when configuring the widgets, perform the following steps and then restart this task from the beginning:

1. Cancel any open wizards in the Operations console.
2. Logon to **LON-AP2**.
3. Open **Internet Explorer** and browse to **http://lon-ap2/DinnerNow** and ensure the **Food Type** and **Meal** drop-down lists are populated. If they are not, close **Internet Explorer** and use the **DinnerNow SQL DB Detacher** from the desktop to re-attach the database,
4. Open **Internet Information Services (IIS) Manager**.
5. Expand **LON-AP2**, expand **Sites**, expand **Default Web Site** and then right-click **DinnerNow**.
6. Click **Manage Application** then click **Browse**.
7. Close **Internet Information Services (IIS) Manager** and the **Internet Explorer** windows.
8. Logoff **LON-AP2**.

**Results:** After this exercise, you should have created a Summary Dashboard view that contains the DinnerNow Database free space in MB and as a percentage. The view also shows the health state of computer running the SQL Server that DinnerNow relies on and any related alerts that are generated on the computer running SQL Server.

## Exercise 7: Configure the SLA Dashboard and publish the dashboard to SharePoint

### Scenario

You have to create an SLA Dashboard for DinnerNow so that IT Management can view service level goals for the DinnerNow .NET Framework applications. The view should also show if the application is meeting its service level goals. Finally, the SLA Dashboard should be published to a SharePoint Portal so that IT Management can access it remotely without having to use the Operations console.

The main tasks for this exercise are as follows:

1. Create the dashboard
2. Publish the dashboard to SharePoint

#### ► Task 1: Create the dashboard

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| Folder   | <b>DinnerNow</b>          |

2. Right-click the **DinnerNow** folder, and then create a new dashboard view by using the following settings (all the other settings should remain the default settings):

- Template: **Service Level Dashboard**
- Name: **DinnerNow SLA**
- SLA to Add: **DinnerNow Web Site**

#### ► Task 2: Publish the dashboard to SharePoint

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                                          |
|----------|------------------------------------------------|
| Computer | <b>LON-AP1</b>                                 |
| Tool     | <b>Internet Explorer</b>                       |
| URL      | <b>http://LON-AP1:8081/SitePages/Home.aspx</b> |
| Link     | <b>Cog icon\Add a Page</b>                     |

2. Add a new SharePoint page by using the following settings (all other settings should remain the default settings):
  - New page name: **DinnerNow\_Availability**.
  - Under Editing Tools, add the **Microsoft System Center** Web Part.
  - Edit the **Web Part**.
  - Operations Manager Web console environments: **Operations Manager Health**.
  - Open a new Internet Explorer tab, and then browse to **http://LON-MS1/Oeprations Manager**.
  - Select the **DinnerNow SLA** dashboard, and then copy the URL from the address bar.
  - Go back to the Web Part and paste the URL into the **Dashboard link** box.
  - Save and close the SharePoint page.
3. On LON-MS1 browse to **http://LON-AP1:8081/SitePages/DinnerNow\_Availability.aspx**.and confirm the DinnerNow SLA Dashboard is displayed.



**Note:** If a 401 Unauthorized page appears close Internet Explorer and then re-open it and browse to [http://lon-AP1:8081/SitePages/DinnerNow\\_Availability.aspx](http://lon-AP1:8081/SitePages/DinnerNow_Availability.aspx)

**Results:** After this exercise, you should have created an SLA Dashboard view that uses the DinnerNow website service level objectives that were previously created. You should then have created a new SharePoint page and added the SLA Dashboard view to the page so that the SLA Dashboard view is available to SharePoint users.

## Exercise 8: Use the GTM tool to publish a custom dashboard

### Scenario

The Windows Server operations team has access only to the Microsoft Windows Servers views in the Operations console. Therefore, you must create a dashboard view that is published to the Microsoft Windows Servers folder. The dashboard should show the performance and availability of all Windows Servers.

The main tasks for this exercise are as follows:

1. Create a new Management Pack
2. Create a new dashboard view
3. Configure the first widget
4. Configure the second widget
5. Configure the third widget
6. Configure the fourth widget
7. Export the Management Pack
8. Copy the GTM tool files and run the tool against the Management Pack
9. Import the Management Pack and view the custom dashboard

#### ► Task 1: Create a new Management Pack

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Management Packs</b>   |

2. Use the **Create Management Pack** task to create a new Management Pack, and use the following settings (all the other settings should remain the default settings):

- Name: **Windows Server Performance Dashboard**

#### ► Task 2: Create a new dashboard view

1. To perform this step, use the computer and the tool information that is shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |

| Location | Value                                       |
|----------|---------------------------------------------|
| View     | <b>Windows Server Performance Dashboard</b> |

2. Create a new Dashboard View and use the following settings (all the other settings should remain the default settings):
- Template: **Grid Layout**
  - Name: **Windows Server Performance**
  - Layout: **4-Cells (select the second layout template)**

#### ► Task 3: Configure the first widget

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                                                   |
|----------|---------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                          |
| Tool     | <b>Operations Console</b>                               |
| Pane     | <b>Monitoring\ Windows Server Performance Dashboard</b> |
| View     | <b>Windows Server Performance</b>                       |

2. Configure the upper-left widget and use the following settings (all the other settings should remain the default settings):
- Template: **Performance Widget**
  - Name: **Memory Utilization**
  - Scope and Counters: Search for Windows Server and then select **Windows Server Computer Group**.
  - Add the following performance counter:
    - Object: **Memory**
    - Counter: **PercentMemoryUsed**
    - Available items: **Select Memory where the Performance Instance column is blank**
  - Time Range: **Last 5 Days**

#### ► Task 4: Configure the second widget

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                   |
|----------|---------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                          |
| Tool     | <b>Operations Console</b>                               |
| Pane     | <b>Monitoring\ Windows Server Performance Dashboard</b> |
| View     | <b>Windows Server Performance</b>                       |

2. Configure the upper-right widget, and use the following settings (all the other settings should remain the default settings):
  - Template: **Performance Widget**
  - Name: **CPU Utilization**
  - Scope and Counters: **Search for Windows Server and then select Windows Server Computer Group.**
  - Add the following performance counter:
    - Object: **Processor Information**
    - Counter: **% Processor Time**
    - Available items: **Select Processor Information where the Performance Instance column displays \_Total**
  - Time Range: **Last 5 Days**

► **Task 5: Configure the third widget**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                   |
|----------|---------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                          |
| Tool     | <b>Operations Console</b>                               |
| Pane     | <b>Monitoring\ Windows Server Performance Dashboard</b> |
| View     | <b>Windows Server Performance</b>                       |

2. Configure the upper-right widget, and then use the following settings (all the other settings should remain the default settings):
  - Template: **Performance Widget**
  - Name: **Logical Disk Free Space (%)**
  - Scope and Counters: **Search for Windows Server and then select Windows Server Computer Group.**
  - Add the following performance counter:
    - Object: **Logical Disk**
    - Counter: **% Free Space**
    - Available items: **Select LogicalDisk where the Performance Instance column displays C:**
  - Time Range: **Last 5 Days**

► **Task 6: Configure the fourth widget**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                   |
|----------|---------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                          |
| Tool     | <b>Operations Console</b>                               |
| Pane     | <b>Monitoring\ Windows Server Performance Dashboard</b> |
| View     | <b>Windows Server Performance</b>                       |

2. Configure the upper-right widget, and use the following settings (all the other settings should remain the default settings):

- Template: **Performance Widget**
- Name: **Processor Queue Length**
- Scope and Counters: **Search for Windows Server and then select Windows Server Computer Group**
- Add the following performance counter:
  - Object: **System**
  - Counter: **Processor Queue Length**
  - Available items: **Select System where the Performance Instance column is blank**
- Time Range: **Last 5 Days**

► **Task 7: Export the Management Pack**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Management Packs</b>   |

2. Create a folder named **Export** on the drive C, and then use the **Export Management Pack** task to export the **Windows Server Performance Dashboard** to the **C:\Export** folder.

► **Task 8: Copy the GTM tool files and run the tool against the Management Pack**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                   |
|----------|-------------------------|
| Computer | <b>LON-MS1</b>          |
| Tool     | <b>Windows Explorer</b> |
| Location | <b>\LON-DC1\Media</b>   |
| Folder   | <b>GTMTool</b>          |

2. Copy the **GTMTool** folder to the **C:\Export** folder on LON-MS1.
3. Open a Command Prompt window, and change to **C:\Export\GTMTool\GTMTool**.
4. Type the following at the command prompt, and then press Enter.

```
GTMTool.exe /SRC C:\Export\Windows.Server.Performance.Dashboard.xml /SRV LON-MS1 /OUT
C:\
```

5. Configure the prompts as follows:
  - GTM Tool Credential Request: **Enter the Contoso\Administrator credentials**
  - Do you want to create a Task Pane Dashboard?: **N**
  - Management Pack Name or **Enter: Microsoft.Windows.Server.Library**
  - Wait for the **Health Monitoring** item to appear, and then enter **Microsoft Windows Server**.
  - Notice the folder where the Management Pack is saved.

► **Task 9: Import the Management Pack and view the custom dashboard**

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Management Packs</b>   |

2. Use the **Import Management Packs** task to import the **Windows.Server.Performance.Dashboard.xml Management Pack** from the **C:\Folder\_0** folder.
3. From the **Monitoring** pane, open the **Microsoft Windows Server** folder, and then view the **Windows Server Performance Dashboard**.

**Results:** After this exercise, you should have created a new Management Pack and dashboard view by using the Grid template. You should have also configured the four widgets to display the performance

counters for all Windows Servers. Then, you exported the Management Pack and used the GTM tool utility to import the Management Pack into the Microsoft Windows Server folder. Finally, you imported the Management Pack, viewed the dashboard, and confirmed that the widgets displayed the correct data.

**Question:** You have to create a dashboard view that contains only critical alerts and alert details. Which template and widgets should you use?

**Question:** You have to create a dashboard view that contains the % Processor Utilization for only computers that run IIS 7. Which template and widget should you use?

## Module Review and Takeaways



**Best Practice:** When you create dashboard views in Operations Manager, you must understand the elements that a dashboard view includes. The dashboard view includes the template that is used to group and display the data, and the widgets that show certain types of data, such as alerts, state, or performance. You must also understand who your audience is for the dashboard. By recognizing the audience, you can make sure that the data focuses on information relevant to this audience.

### Review Question(s)

**Question:** You have created a Summary Dashboard view that displays the health and performance for a line-of-business web application. You have to make the view available to other personnel in the organization who do not have access to the Operations console or the Web console. You have SharePoint 2010 installed. What should you do?

### Tools

#### GTM Tool

The GTM tool can be used to add dashboard views to any Management Pack folder. It can also be used to create a context-sensitive task that opens a dashboard view that is based on selected objects in the Operations console. The GTM tool can be downloaded from here:

<http://go.microsoft.com/fwlink/?LinkID=321901>



# Module 8

## Configuring and Customizing the Operations Console

### Contents:

|                                                                    |             |
|--------------------------------------------------------------------|-------------|
| Module Overview                                                    | 8-1         |
| <b>Lesson 1: Security, Scoping, and User Roles</b>                 | <b>8-2</b>  |
| <b>Lesson 2: Creating Custom Views and Alert Resolution States</b> | <b>8-7</b>  |
| <b>Lesson 3: Configuring Notification Subscriptions</b>            | <b>8-12</b> |
| <b>Lesson 4: Creating Diagnostic and Recovery Tasks</b>            | <b>8-17</b> |
| <b>Lab: Customizing the Operations Console</b>                     | <b>8-22</b> |
| Module Review and Takeaways                                        | 8-38        |

## Module Overview

Application support teams that use Microsoft System Center 2012 R2 Operations Manager can do so either via a locally installed console or through the Web console. Typically within an application support team, a number of roles require different levels of permissions to use the Operations console. These roles range from read-only users to advanced operators. In addition, all of these user roles must be configured to display only data about the computers and applications that the users are responsible for. In this module, you will learn how to use the built-in, role-based security within Operations Manager to provide granular access to data, views, and tasks in Operations Manager.

Application support teams typically require customized views within the console for their key applications. You will also learn how to design and provision these views to relevant support teams.

Although some team members might always have the console open and thus be aware of issues when they arise, other teams might not always have access to the console and thus require a notification be sent when an issue is detected. Operations manager uses notifications and notification channels to achieve this functionality. This module describes how to configure these and send email alerts to the relevant teams.

Finally, to reduce workload on the various application support teams, you will learn how to configure diagnostic and recovery tasks in Operations Manager so that you can diagnose and automate the remediation of detected issues.

### Objectives

After completing this module, students will be able to:

- Configure security, scoping, and user roles.
- Create custom views.
- Configure notification subscriptions.
- Create diagnostic and recovery tasks.

## Lesson 1

# Security, Scoping, and User Roles

Security in the Operations console is managed by using user roles. A *user role* is a combination of a profile and scope. The *profile* determines what operations can be performed, and the *scope* determines which objects operations can be performed on. A number of built-in user profiles, such as read-only operator and advanced operator profiles, can be used to scope what can be viewed and accessed in the Operations console.

It is important that you understand how user roles are configured in Operations Manager so that you can control who has access to the Operations console, what actions they can perform, and on which objects they can perform those actions.

### Lesson Objectives

After completing this lesson, students will be able to:

- Describe user roles in Operations Manager.
- Configure user roles in Operations Manager.

### Overview of User Roles in Operations Manager

You can access Operations Manager 2012 by using the Operations console, the Web console, Windows PowerShell, or custom applications. The level of access in Operations Manager is controlled by membership to one or more user roles and their accumulated rights.

Operations Manager 2012 can monitor many kinds of applications in the environment. Typically, these applications are managed by multiple teams in the organization. As the Operations Manager administrator, you can limit access to each team, and each team can access only monitored data that is relevant for that team. Role-based security lets you grant access to monitored data, views, and tasks on a team-by-team basis.

#### Operations Manager user roles:

- Administrator
- Advanced Operator
- Application Monitoring Operator
- Author
- Operator
- Read-Only Operator
- Report Operator
- Report Security Administrator

To help you understand how role-based security works in Operations Manager, consider the following terminology:

- **Operation/Privilege.** A securable action, such as resolving alerts, executing tasks, overriding monitors, creating user roles, viewing alerts, and viewing events.
- **Profile.** A collection of operations that are granted to a persona, for example, Administrator or Operator.
- **Scope.** Defines the boundaries of the running of profile operations, for example, tasks and groups.
- **Role Assignment.** An association of Windows users and groups to Operations Manager roles.
- **User Role.** In Operations Manager, a user role is created by defining a union of profile and scope. You create a user role from one of the five predefined profiles, or one of the eight predefined profiles if Reporting is installed, and then define an appropriate scope.

The following table describes each profile type, and an appropriate scope for each type.

| Profile type                    | Description                                                                                                                                                                                                                  | Scope                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator                   | The Administrator profile has full permissions in Operations Manager. This includes access to all Operations Manager data and functions that are provided in the Administration and Authoring workspaces.                    | No scoping of the Administrator profile is supported.                                                                                                                |
| Advanced Operator               | The Advanced Operator profile provides restricted change access in Operations Manager. This includes the ability to create overrides to monitors and rules to which the profile is scoped.                                   | The Advanced Operator profile can be scoped against views, tasks and groups.                                                                                         |
| Application Monitoring Operator | The Application Monitoring Operator profile is used to provide access to the Application Monitoring events in the Application Diagnostics web console.                                                                       | This profile is created during setup and is globally scoped against Users or Groups.                                                                                 |
| Author                          | <ul style="list-style-type: none"> <li>• The Author profile lets you edit, delete, and create the following objects in Operations Manager:</li> <li>• Rules</li> <li>• Monitors</li> <li>• Views</li> <li>• Tasks</li> </ul> | The Author profile can be scoped against groups, views, and tasks. Additionally, it is the only profile that can be scoped against any target in Operations Manager. |
| Operator                        | The Operator profile can be used to provide edit and delete functions for alerts based on its scope. This profile can also be used to provide access to views and tasks based on its scope.                                  | The Operator profile can be scoped against views, groups, and tasks.                                                                                                 |
| Read-Only Operator              | The Read-Only Operator profile can be used to view alerts and access views based on its configured scope.                                                                                                                    | The Read-Only Operator profile can be scoped against groups and views.                                                                                               |
| Report Operator                 | The Report Operator profile can be used to view reports that are based on its configured scope.                                                                                                                              | Globally scoped.                                                                                                                                                     |
| Report Security Administrator   | The Report Security Administrator profile is used to integrate the security of Microsoft SQL Server Reporting Services with roles in Operations Manager.                                                                     | No scope.                                                                                                                                                            |

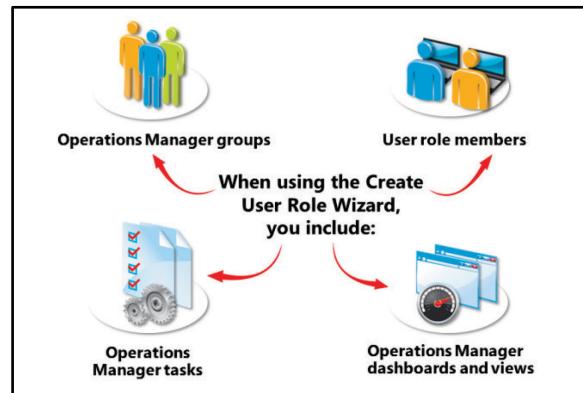
You can create new user roles in Operations Manager by using the Create User Role Wizard. Each user role is a combination of a profile and scope, as previously described. When you create a user role, you select a relevant profile such as Author, and then you define the scope. The scope determines the objects that members of the user role will have access to.

For example, you might create a user role named SQL Admins that is based on the Advanced Operator profile. You can then include a scope that contains only instances of SQL Server and the views and tasks that will be made available to members of this user role. Finally, you can add the relevant Active Directory user accounts as members of the user role. When a member of this user role opens the Operations console or Web console, he or she will view and have access only to the instances of SQL Server and the views and tasks that are defined in the scope.

## The Process of Configuring User Roles in Operations Manager

To understand how user roles are configured in Operations Manager, it is helpful to consider a scenario. In the following scenario, you identify the kind of access required and for whom, and then review the process for configuring that access. The following list outlines your requirements:

- In your organization, you have a dedicated team of Windows Server operators that manage the Windows Server platform.
- You also have a dedicated team of SQL Server operators that manage deployments of SQL Server.
- Both teams require access to the Operations console to monitor the Windows Server and SQL Server platforms.
- When using the Operations console, the SQL Server team must not be able to view alerts or perform tasks on the Windows Servers.
- When using the Operations console, the Windows Server team must not be able to view alerts or perform tasks that relate to SQL Server.



To facilitate proper access, you would perform the following steps:

1. Create an Active Directory group for each team, and then add the relevant user accounts to these groups in Active Directory. For example, the Active Directory group named SQL\_Admins includes the SQL Server operator team members. The Active Directory group named Windows\_Admins includes the Windows Server operator team members.
2. In the Operations console, from the User Roles node in the Security section of the Administration pane, you create a new Operator user role. Described in the following table are the pages of the Create User Role Wizard that are used to create a user role for the SQL Server operators.

| Create User Role Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties           | Specify the user role name as it will be displayed in the Operations console. In the scenario described in the preceding list, you add a user role name of SQL Administrators. You also add the Active Directory Users or Groups that will be included in this User Role. In this scenario, you add the SQL_Admins Active directory group.                                                                                                                                                                                        |
| Group Scope                  | <ul style="list-style-type: none"> <li>Select the Operations Manager Groups that members of the user role will have access to and potentially perform administrative tasks against. In this scenario, you select only the following groups:</li> <li>SQL Server 2012 Computers</li> <li>SQL Server 2012 DB Engine</li> <li>SQL Server 2012 Replication Computers</li> </ul>                                                                                                                                                       |
| Tasks                        | Add the Operations Manager tasks that member of the user role will be able to perform. When adding the tasks, a Select Tasks window displays all available tasks. You can order the tasks so that they are displayed by Management Pack. This ability to arrange tasks is useful because you can select all tasks related to something specific; for example, in this scenario, you can select all tasks that relate to the SQL Server 2012 (Monitoring) Management Pack. Note that Console tasks cannot be scoped in user roles. |
| Dashboards And Views         | Select the Operations Manager views available to members of the user role in the Operations console. In this scenario, you select only the Microsoft SQL Server folder. This contains all the SQL Server views and will be selected by default. You also add any relevant dashboards that should be made available in the Tasks pane.                                                                                                                                                                                             |
| Summary                      | Review the properties of the user role that will be created, including the user role members, groups, tasks, and views. You can go back through the wizard if necessary and make relevant changes before clicking the Create button to create the user role.                                                                                                                                                                                                                                                                      |

3. After creating the user role, the role is displayed in the User Roles node in the Operations console, where you can edit it. You might need to edit the user role if you add views to the folder, for example. After you edit the user role, you select the additional views on the Dashboards And Views tab.

When a member of the SQL Administrators user role opens the Operations console, that member's view is scoped based on the selections defined when the user role was created. For example, only the views contained in the Microsoft SQL Server folder would be available as mentioned in the table above. This means that the Active Alerts view in the Microsoft SQL Server folder displays only alerts relating to the SQL role. Similarly, the Computers view displays only computers running SQL Server.

To configure the user role for the Windows Server operators, you would follow the same procedure as just described, but instead you would select the relevant Windows Server groups, views, tasks, and dashboards.

 **Note:** You can also create a new User Role by using the Add-SCOMUserRole PowerShell Cmdlet. The following command creates a new User Role named *DinnerNow Operators* and associates it with the *Read Only Operator* profile:

```
Add-SCOMUserRole -Name 'DinnerNow Operators' -ReadOnlyOperator
```

For more information about configuring User Roles in Operations Manager visit the following website.

#### **Implementing User Roles**

<http://go.microsoft.com/fwlink/?LinkId=404091>

## Demonstration: Configuring a User Role

In this demonstration you will learn how to configure a User Role by using the Operations Console.

### Demonstration Steps

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                      |
|----------|----------------------------|
| Computer | <b>LON-MS1</b>             |
| Tool     | <b>Operations Console</b>  |
| Pane     | <b>Administration</b>      |
| View     | <b>Security\User Roles</b> |

2. Use the Create User Role Wizard to create a user role by using the following settings (all other settings should remain the default settings):
  - Profile: **Operator**
  - User role name: **Demo**
  - User role members: **Contoso\SQL\_Admins**
  - Group Scope: Select all groups that are prefixed with **SQL**
  - Tasks: Add all tasks that belong to Management Packs that begin with **SQL**
  - Dashboards and Views: On the **Monitoring Tree** tab, add the **Microsoft SQL Server** folder, and then ensure all subfolders and views are also added

**Question:** What profile has the least privileges required to create overrides in Operations Manager?

## Lesson 2

# Creating Custom Views and Alert Resolution States

When you install Management Packs in Operations Manager, monitoring views are automatically created within the Monitoring pane. These views are configured to display data for the application that the Management Pack was designed to monitor. You can also create your own views to display other data that Operations Manager has collected. These can be created in your own personal workspace or, if you have the required permissions, in the Monitoring pane for others to view. You can create views that include data such as performance, state, or alert data.

You should understand how to create custom views in Operations Manager so that operators can view the data they need when monitoring applications and services in your environment.

## Lesson Objectives

After completing this lesson, students will be able to:

- Describe the various views that can be created in the Operations console.
- Configure views in the Operations console.
- Configuring alert resolution states in the Operations console.

## Operations Manager Views

Depending on the Management Packs that have been deployed in Operations Manager, the number of views available in the Operations console will differ greatly. For example, after importing the Management Pack for SQL Server, the following views and folders, which contain multiple views, become available from within the Microsoft SQL Server folder in the Monitoring pane of the Operations console:

- Active Alerts
- Computers
- Tasks Status
- AlwaysOn High Availability
- Databases
- Health Monitoring
- Mirroring
- Performance
- Replication
- Server Roles
- SQL Agent

**Operations Manager provides the following view types:**

- Alert view
- Event view
- State view
- Performance view
- Diagram view
- Task Status view
- Web Page view
- Dashboard view
- Overrides Summary view

Views within the Monitoring pane provide the key monitoring indicators for an application or service being monitored by Operations Manager. There are nine view types that can be created in Operations

Manager. Included in the following table is a description of each view type, including a typical example of how the views are used in the Operations console.

| Operations Manager view type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alert view                   | Used to display alerts that Operations Manager has generated. This view can be used to display alerts with a specific criterion—for example, alerts that have a high priority or alerts that were generated within a specific time period such as within the last two hours. A typical example of when to use an Alert View is when you want to display alerts that have a high priority, have a severity of critical, and are in a new resolution state for an application or service being monitored by Operations Manager.                                                                                                                                                     |
| Event view                   | Used to display events that have been collected by Operations Manager. For example, you could create an NT Event Log collection rule to collect events relating to a line-of-business web application. An Event View can then be used to view these events.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| State view                   | Used to display the health state of a monitored entity in Operations Manager. For example, you can create a State View that displays the health state of Windows-based computers that a line-of-business web application is hosted on.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Performance view             | Used to display performance data that has been collected by Operations Manager and stored in the operational database. For example, you can create a Windows Performance Collection Rule that collects performance data relating to a line-of-business web application, and then use a Performance view to view the performance data collected. When using the Performance view, you select the performance counters to display in the graph. You can adjust the time frame of data displayed to enable you to pinpoint a specific time. This is useful when you need to correlate performance data with events that have occurred in the environment, such as a website failure. |
| Diagram view                 | Used to display the monitored components of an application or service monitored by Operations Manager. Similar to a Distributed Application Diagram, this view displays each monitored object, including its relationship to other objects within the view. The Diagram view can be used to display, in a single view, the health state of monitored objects such as the database, website, and operating system of a monitored application.                                                                                                                                                                                                                                      |
| Task Status view             | Used to display the status of tasks performed against managed objects in Operations Manager. This provides a method of filtering the tasks displayed in the Task Status view in the Monitoring pane. This view can be used to display the task status of all tasks run against a specific computer, such as an application server. You can use criteria to filter the list of returned task statuses, such as tasks of a specific state or run by a specific account.                                                                                                                                                                                                             |
| Web Page view                | Used to display a website within a view in the Operations console. This can be useful when you need to verify a webpage is available by viewing it in the console, for example, the status page of a line-of-business web application. The webpage is displayed in the view as if you opened it in a browser, and you can browse the page just as you would if viewing it through a web browser.                                                                                                                                                                                                                                                                                  |
| Dashboard view               | Used to create a dashboard based on the widgets and template selected when configuring the dashboard. This feature was covered in detail in                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Operations Manager view type | Description                                                                                                                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | the Lesson titled “Dashboards and Widgets” in Module 7, “Scorecards, Dashboards, and Reporting.”                                                                                                                                               |
| Overrides Summary view       | Used to view the overrides that have been created for rules and monitors in Operations Manager. You can use this view to view overrides for both sealed and unsealed Management Packs. This view is available only from the My Workspace pane. |

## The Process of Configuring Views in Operations Manager

Views can be created in the Monitoring pane of the Operations console. You can create a view that is made available from the top-level node in the Monitoring pane by right-clicking the Monitoring node and then clicking New. The nine view types described in the previous topic are then made available. You can also create a view from any folder that belongs to an unsealed Management Pack in the same manner. For folders that belong to a sealed Management Pack, such as the Microsoft SQL Server folder, the New option is not available.

**When configuring a view in Operations Manager, you specify:**

- The view name
- The criteria for the view
- The data target
- The group that contains the data to be displayed

You can also create a new folder in the Monitoring pane to store views. This is useful when you want to group a number of views for an application, for example.

Unless filtered out by a user role, any view that you create in the Monitoring pane will be made available to all users of the Operations console. This is useful when you need to create views that all operators should be able to use. If you want to create a view that only you have access to in the Operations console, create this view in the My Workspace pane. In the same way you can create folders and views in the Monitoring pane, you can create folders and views in the My Workspace pane, and they are only visible to you. This is useful when you need to create a temporary view or a view that contains data that only you should view.

Views that you create in the Monitoring pane are also made available in the Web console. This is also true for views created in the My Workspace pane.

### Configuring Views

When configuring views in Operations Manager, in most cases, four elements of the view must be configured:

- **Name.** You provide the descriptive name for the view that will be displayed in the Operations and Web consoles. You can optionally include a description.
- **Criteria.** You can filter the view based on selected criteria. Criteria differ based on the view being created. For example, when creating an Event view, criteria such as the event number and source can be used to filter the data returned in the view. You select the criteria to use, and then either select or enter in the criteria to be used. For example, when selecting the event number criteria, you must type the event number to filter on. Conversely, when choosing the severity level criteria, you can select from various severity levels to filter on.

- **Show Data Related To.** You select the class, group, or object that should be used as the target for the view being created. For example, if you wanted to display all performance counters collected for all SQL databases, you would select the SQL Databases class. When selecting the class, group, or object, you can search through all targets or just common targets, which is useful when you know some or all of the target name—for example, SQL.
- **Show Data Contained In A Specific Group.** You select a group from which the targeted data will be displayed. You can select all groups from here or, if you need to retrieve data from a specific instance or group of computers, you can select the relevant group.

After the view is created, the view will immediately start to display data based on the four elements described in the preceding list. You can edit the properties of the view if, for example, you need to change the criteria. This is useful because you might need to change elements of the view, such as the target or computer group.

For more information about creating views in Operations Manager visit the following website.

#### **Creating Views in Operations Manager**

<http://go.microsoft.com/fwlink/?LinkId=404092>

## The Process of Configuring Alert Resolution States

Alert resolution states in Operations Manager provide a method of assigning alerts to specific teams or personnel. When you right-click an alert in Operations Manager, the Set Resolution State option allows you to assign the alert to any resolution state configured in Operations Manager.

This is useful in many organizations in which there are different levels of support such as 1<sup>st</sup> Line, 2<sup>nd</sup> Line, and 3<sup>rd</sup> Line Support. By configuring alert resolution states for these support teams, you can assign or escalate alerts to them based on the

alert's severity, priority, and criticality. Furthermore, as mentioned in the previous topic, you can create a custom alert view that is based on the alert resolution state. This means, for example, that 3<sup>rd</sup> Line Support personnel can have a view that displays only alerts assigned to 3<sup>rd</sup> Line Support. This way, support teams work only on alerts that are assigned to them.

Alert resolution states can also be used with notification subscriptions to filter the types of alert that are sent as notifications.

Each resolution state in Operations Manager has a unique ID associated with it. For example, new alerts have a resolution state ID of 0, whereas alerts that are closed have a resolution state ID of 255.

### **Creating Alert Resolution States**

To create a new alert resolution state, you go to the Settings node in the Administration pane of the Operations console to edit the properties of the Alerts setting. When you edit the properties, the Global Management Group Settings – Alerts dialog box opens, where the Alert Resolution States tab displays all configured alert resolution states, including their IDs.

To create a new alert resolution state, click New. You then provide a resolution state name such as 3<sup>rd</sup> Line Support and a unique ID such as 55. You can use any ID in the range of 1 through 253, excluding IDs that

#### **Alert resolution states can be used to:**

- Assign alerts to the most appropriate operators
- Manage alerts in the Operations console
- Filter alert views for specific operators such as 3<sup>rd</sup> Line Support operators
- Filter notification subscriptions

have already been used by other alert resolution states. Typically, you should not use any ID above 240, because these are often used by Microsoft.

After you save the new alert resolution state, when you use the Set Resolution State option on the alert, the alert resolution state becomes immediately available.

When you use alert resolution states, you can help manage alerts in the Operations console by assigning the alerts to the most appropriate operators.



**Note:** You can also create new Alert Resolution States by using the Add-SCOMAlertResolutionState PowerShell Cmdlet. The following command creates a new Alert Resolution State named *DinnerNow* and sets the resolution state code to 33:

```
Add-SCOMAlertResolutionState -Name "DinnerNow" -ResolutionStateCode 33
```

Verify the correctness of the statement by placing a mark in the column to the right.

| Statement                                                                              | Answer |
|----------------------------------------------------------------------------------------|--------|
| When you create a view in the Monitoring pane, the view is made available only to you. |        |

## Lesson 3

# Configuring Notification Subscriptions

Notifications are used within Operations Manager to send alerts to specific users via specific channels (for example, email). From both a technical and a business perspective, you need to define for which alerts a notification is required and the type of notification that should be sent. For example, a business-critical application alert might require a Short Message Service (SMS) notification to be sent regardless of when the issue occurs. Conversely, when a nonbusiness-critical alert occurs, a standard email notification might suffice.

You can also configure custom resolution states within Operations Manager. These allow you to filter both views and notification subscriptions based upon specific states in Operations Manager. You would consider configuring custom resolution states to allow an alert to be escalated to another team.

In this lesson, you learn how to configure notifications in Operations Manager.

### Lesson Objectives

After completing this lesson, students will be able to:

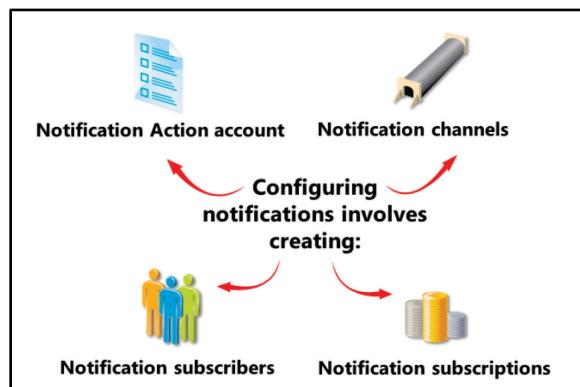
- Explain notifications in Operations Manager.
- Configure notification channels.
- Configure notification subscribers.
- Configure notification subscriptions.

### Overview of Notifications in Operations Manager

Notifications are used to send messages or run commands that are based on specific alerts generated in Operations Manager.

Notifications can be sent by using different methods such as sending email, a text message (SMS), or an instant message (IM). A notification can also use a command, which can be useful when you use a third-party notification application and device such as a pager.

The four steps for configuring notifications in Operations Manager are described in detail in the following table.



| Notification step                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create and configure the notification action account | The Notification Action account is used to provide credentials when you send notifications. The account must be created and configured by an Operations Manager administrator. This involves creating a Run As account and associating it with the Notification Account Run As profile. After you create the Run As account, you must edit the Distribution settings and click the More Secure option to target the computers to which the account will be distributed, such as the Operations Manager Management Servers. |
| Configure the Notification                           | The notification channel must be created by an Operations                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Notification step                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Channel                                 | Manager administrator. Depending on the channel you are creating, different settings have to be configured. For example, the email notification channel requires the Simple Network Management Protocol (SMTP) server details and a return address. The command channel requires the full path of the command file and the command-line parameters.                                                                                                                                                                                                                                                                                                                                                                              |
| Configure the Notification Subscriber   | A notification subscriber can be created by an Operations Manager administrator, an advanced operator, and an operator. Standard operators of the Operations console can determine whether to create subscriptions from an alert in the Operations console. When you configure the notification subscriber, you can set a master notification schedule of when notifications will be sent, such as weekdays or weekends. Then you add the subscriber address. This address is a combination of a channel and a schedule, and allows for different notification types to be used at different times. For example, an email notification can be sent during working hours, and an SMS message can be sent during nonworking hours. |
| Configure the notification subscription | A notification subscription can be created by an Operations Manager administrator, an advanced operator, and an operator. A notification subscription defines the criteria for a notification, such as whether the notification will address critical alerts or alerts with a specific priority. The channel to be used by the notification, and the subscriber to receive the notification, are also defined in a notification subscription.                                                                                                                                                                                                                                                                                    |

## How Notification Channels Are Configured

Notification channels can be viewed in the Channels view of the Notifications node in the Administration pane of the Operations console. To create a channel, you click the New task that is available in the Tasks pane. This opens a dialog box in which you select the channel that you want to create.

The following table describes the key settings that are configured for each notification channel.

### Notifications can be sent by:

- Email
- Instant message (IM)
- Text message (SMS)
- Command

| Notification channel | Setting      | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Email                | SMTP Servers | <p>You must add a minimum of one SMTP server fully qualified domain name (FQDN) that will be used to send email notifications. Adding multiple SMTP servers provides failover. The failover order can also be configured.</p> <p>The return address is also required. Typically, this is the email address of the account that is used when the Notification Action account is being created. However, a mailbox address does not have to be associated with the</p> |

| Notification channel | Setting                       | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |                               | <p>email address.<br/>A retry interval can also be configured. The default interval is five minutes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                      | Format                        | The email message format can be configured to include the subject, email message, and importance. In this way, you can customize the data that is included in the email. For example, you can add custom alert fields such as operator comments or troubleshooting steps that were taken. By default, a link to the alert in the Operations Manager Web console is included in the message content. Other fields that can be added to the subject and message include Alert Severity, Alert Priority, and Alert Raised Time. |
| Instant Message (IM) | IM Server                     | The FQDN of the instant message (IM) server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                      | Return Address                | The return address must be prefixed with <i>sip</i> (Session Initiation Protocol). Typically, this is the address of the account that is used when the Notification Action account is created, and it is a Session Initiation Protocol (SIP) enabled account in Active Directory Domain Services (AD DS). The protocol, authentication method, and IM port are also configured.                                                                                                                                              |
|                      | Format                        | The IM message format can include several fields, such as Alert Security and Alert Priority. Custom fields can also be added.                                                                                                                                                                                                                                                                                                                                                                                                |
| Text Message (SMS)   | Text Message                  | Typically, the text message is kept short and includes only the minimum required information. By default, the Alert Name and Resolution State fields are added. However, other fields can be included.                                                                                                                                                                                                                                                                                                                       |
| Command              | Full Path Of The Command File | This includes the path and the file name of the command file that should be run as part of the notification. Parameters should not be included here and will cause the notification to fail.                                                                                                                                                                                                                                                                                                                                 |
|                      | Command Line Parameters       | Any parameters for the command file are included here. This can also include alert fields such as Alert Severity and Alert Priority.                                                                                                                                                                                                                                                                                                                                                                                         |



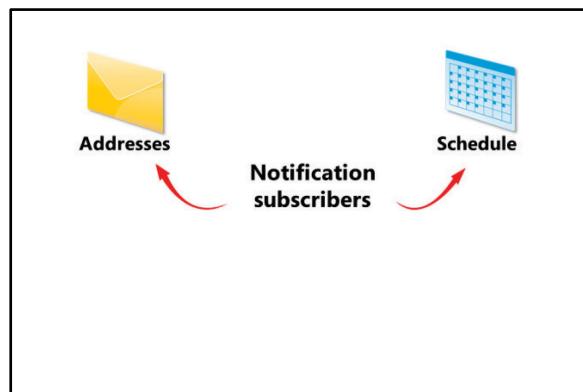
**Note:** You can also create a Notification Channel by using the Add-SCOMNotificationChannel PowerShell Cmdlet. The commands in the example below create a new IM Notification Channel named *IM Channel*:

```
$Body = "SCOM alert `"$Data[Default='Not Present']/Context/DataItem/AlertName`$"
Add-SCOMNotificationChannel -Name "IM Channel" -Server "SIP.contoso.com" -UserName
'sip:Admin' -Body $Body
```

## How Notification Subscribers Are Configured

If you are a member of the Operations Manager administrators' user role, you can configure subscribers in the Notifications node, in the Administration pane. If you are an Operations Manager operator or advanced operator, the Administration pane is not available because of the restrictions applied to these roles. An operator or advanced operator can use the Tools menu in the Operations console, where the My Subscriber Information and My Subscriptions options are available.

When you configure a subscriber, you configure the settings described in the following table.



| Subscriber setting | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schedule           | By default, notifications can be sent at any time. Alternatively, you can add a schedule with a date range by using a From and To date, and a Weekly Recurrence. For example, you could configure the range to Monday through Friday between 9:00 A.M. and 5:00 P.M. Multiple schedules with different settings can be added to provide fine-grained control when notifications are sent.                                                                                                                                                                                             |
| Addresses          | The address is a combination of the address name and the channel, such as SMTP, and includes the delivery address and the schedule. By adding multiple addresses and schedules, you can use different notification channels at different times of the day.<br><br>For example, during the day, you might have access to email. But after 5:00 P.M., you do not. You can create a schedule to use the email channel between 9:00 A.M. and 5:00 P.M. Another schedule can be created to use the SMS channel after 5:00 P.M. so that you can send a text message to your cellular phone. |

 **Note:** You can also create Notification Subscribers by using the Add-SCOMNotificationSubscriber PowerShell Cmdlet. The following command creates a Notification Subscriber which includes addresses for email, SMS and IM:

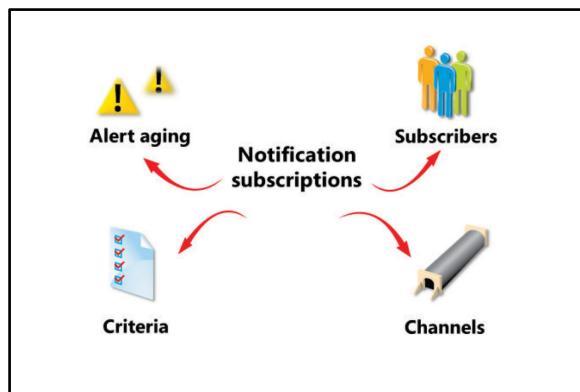
```
Add-SCOMNotificationSubscriber -Name "Andrew Jenkins" -DeviceList
"AndrewJ@contoso.com", "sms:2065551212", "sip:AndrewJ"
```

## How Notification Subscriptions Are Configured

When you log on to the Operations console as an administrator, you can configure subscriptions from the Administration pane in the Notifications node. When you log on to the Operations console as an operator or advanced operator, you create subscriptions by using the My Subscriptions option on the Tools menu.

Additionally, subscriptions can be configured by right-clicking an alert in the Operations console. The Notification Subscription option becomes available, where you can create a new subscription or change an existing subscription. This feature is especially useful because Operations Manager automatically configures the subscription criteria for you based on the alert that is selected.

When you configure a notification subscription, the settings described in the following table are available.



| Subscription setting | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Criteria             | You configure the conditions that you will use as criteria to determine the alerts that will be forwarded as notifications. Several conditions can be used, such as Of A Specific Severity and With A Specific Name. The Created By Specific Rules Or Monitors condition is useful because you can target any rule or monitor from any Management Pack and send a notification based on an alert that is generated by that rule or monitor. Multiple conditions can be added to build a list of criteria by using the AND operator. For example, if you add the With A Specific Resolution State and With A Specific Ticket ID Conditions criteria, a notification is sent when an alert matches the configured resolution state and has the configured ticket ID.                                                                                                         |
| Subscribers          | When you configure a subscription as an Operations Manager administrator, you can either add an existing subscriber or create a new one. When you configure a subscription as an Operations Manager operator or advanced operator, the subscriber information is already included. Although this information can be edited, a new subscriber cannot be added.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Channels             | As an Operations Manager administrator, you can create a new channel, add or edit an existing channel, or create a customized copy of an existing channel. This is useful if you make a small change to an existing channel and do not have to change every setting. For example, you might have an email channel that is used to send email notifications with a specific set of alert fields included in the message. By using the Create Customized Copy option, you can create a new channel that is based on the existing channel and then change the alert fields included in the message. Then, Operations Manager creates a new channel with these settings. Operations Manager operators and advanced operators can add existing channels and create customized copies of existing channels with limited customization. However, they cannot create new channels. |
| Alert Aging          | Alert aging can be used to delay notifications before they are sent. This is useful when an alert is resolved in a defined number of minutes. For example, when a server is restarted, you could add a delay of five minutes so that notification is sent only if the server is unavailable for more than five minutes. If the server restarts as expected, the alert automatically will be resolved. By default, notifications are sent without any delay.                                                                                                                                                                                                                                                                                                                                                                                                                |



**Note:** You can also create a new Notification Subscription by using the Add-SCOMNotificationSubscription PowerShell Cmdlet. The following commands create a Notification Subscription named *CriticalDinnerNowAlerts*:

```
$Subscriber = Get-SCOMNotificationSubscriber -Name "Andrew Jenkins"
$Channel = Get-SCOMNotificationChannel -DisplayName "Email"
Add-SCOMNotificationSubscription -Name "CriticalDinnerNowAlerts" -Subscriber
$Subscriber -Channel $Channel
```

**Question:** You must create a notification subscription for an alert that is generated in the Operations console. What is the easiest method to achieve this notification subscription?

## Lesson 4

# Creating Diagnostic and Recovery Tasks

When an issue is detected by Operations Manager, a diagnostic or recovery task can be started. A *diagnostic task* executes a command or script and then embeds the output in the Operations Manager Health Explorer to help with troubleshooting the issue. A *recovery task* runs a command or script and then attempts to automatically resolve the issue.

For example, suppose you have a monitor that monitors the health state of a Windows service. If the service stops unexpectedly, the health state of the monitor changes to a warning or critical state. You can add a recovery task that automatically tries to restart the service. Recovery tasks are used to automatically fix a detected issue, and diagnostic tasks are used to diagnose a detected issue and provide more information about the root cause.

To provide root cause analysis and automate remediation, it is important that you understand how to create diagnostic and recovery tasks in Operations Manager.

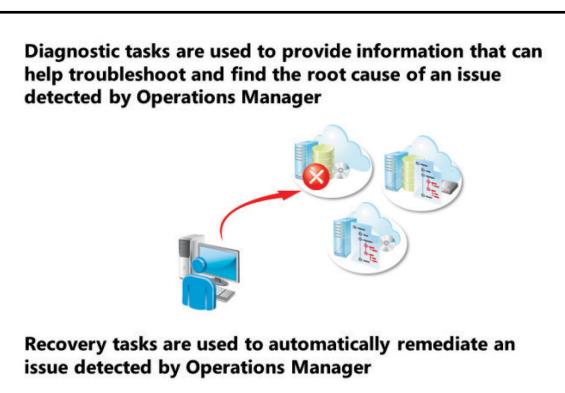
### Lesson Objectives

After completing this lesson, students will be able to:

- Describe diagnostic and recovery tasks in Operations Manager.
- Configure recovery tasks in Operations Manager.

### Overview of Diagnostic and Recovery Tasks

Diagnostic and recovery tasks can be configured to run automatically when a monitor changes its health state. For example, when a monitor changes from healthy (green) to warning (yellow), a diagnostic task can be started automatically to collect information to help the operator diagnose the issue. Diagnostic and recovery tasks can also be configured to be run manually by an operator who is investigating the issue detected by the monitor. In this case, after the operator selects the monitor, the operator clicks the task on the State Change Events tab in the Operations Manager Health Explorer.



To understand how monitors use diagnostic and recovery tasks, consider a good example of a monitor, such as the Health Service Heartbeat Failure monitor, which is automatically included with Operations Manager and checks the availability of every System Center Management Service in the Management Group. When viewing the properties of this monitor, the Diagnostic And Recovery tab shows any diagnostic and recovery tasks configured for the monitor. For example, two diagnostic tasks associated with the Health Service Heartbeat Failure monitor are both configured to run automatically as described here:

- **Ping Computer On Heartbeat Failure.** This task pings the affected computer to determine whether it is responding to a TCP/IP connection by using Internet Control Message Protocol (ICMP).
- **Check If Health Service Is Running.** This task checks to determine whether the health service is running on the computer that generated the alert.

Seven recovery tasks are also associated with this monitor as described in the following list:

- **Reinstall Health Service (triggered from Diagnostic).** This task reinstalls the Health service on the computer that generated the alert after the Check Health Service Service Control Manager Configuration diagnostic task has been run.
- **Reinstall Health Service Manually.** This manual task reinstalls the Health service on the computer that generated the alert.
- **Resume Health Service.** This manual task resumes a paused Health service.
- **Enable and Restart Health Service.** This manual task enables the Health service if it has been disabled on the computer that generated the alert and then restarts it.
- **Set The “Computer Not Reachable” Monitor To Success Because The “Ping Computer On Heartbeat Failure” Diagnostic Succeeded.** This automatic task sets the Computer Not Reachable monitor to success when the Ping Computer On Heartbeat Failure diagnostic task succeeds.
- **Restart Health Service.** This manual task restarts a stopped Health service on the computer that generated the alert.
- **Reserved (Computer Not Reachable – Critical).** This is a reserved task that cannot be modified or removed.

To understand how these diagnostic and recovery tasks are used, consider the following scenario:

- An agent-managed computer is turned off unexpectedly as a result of a power outage.
- In the Operations console, a Health Service Heartbeat Failure alert is generated.
- You investigate the alert by opening the Operations Manager Health Explorer.

In the Operations Manager Health Explorer, you select the Health Service Heartbeat Failure alert and then click the State Change Events tab. From the Details section, you can view the diagnostic and recovery tasks that were run automatically and review any output that was generated. You can manually run the Check If Health Service Is Running and Ping Computer On Heartbeat Failure diagnostic tasks by clicking the available links in the Details section. You can also run recovery tasks, such as the Restart Health Service and Enable And Restart Health Service tasks, by clicking the relevant links.

For each diagnostic and recovery task that was run either manually or automatically, results are automatically appended in the Details section. These results include the status of the task, the date and time the task was run, the user who submitted the task, and any diagnostic or recovery output generated by the task. This information makes troubleshooting an unhealthy monitor much a quicker and easier process, because you do not need to navigate away from the State Change Events tab to perform common troubleshooting tasks.

For more information about Diagnostic and Recovery tasks in Operations Manager visit the following website.



## Diagnostic and Recovery Tasks

<http://go.microsoft.com/fwlink/?LinkId=404093>

## How Diagnostic and Recovery Tasks Are Configured

You configure diagnostic and recovery tasks for a monitor by editing the monitor's properties. In the monitor properties dialog box, on the Diagnostic And Recovery tab, the diagnostic tasks are displayed in the top section, and the recovery tasks are displayed in the bottom section. To create a diagnostic or recovery task, you click the Add button in either the Diagnostics or Recoveries section.

After clicking Add, you must specify whether the diagnostic or recovery task should be triggered based on a warning or critical health state. For example, if you clicked the Recovery For Warning Health State option, the recovery task would be run when the health state of the monitor changed to warning. After selecting the health state, if creating a diagnostic task, the Create Diagnostic Task Wizard starts. If creating a recovery task, the Create Recovery Task Wizard starts. Described in the following table are the pages and settings of the Create Diagnostic Task Wizard.

**When configuring a diagnostic or recovery task, you include:**

- The command or script to run
- The Management Pack where the task should be saved
- Any parameters that should be included with the command or script
- Whether the task should be run automatically or manually

| Create Diagnostic Task Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Diagnostic Task Type               | Select the type of task that will be run. This can be either a command or a script file. You also specify the unsealed Management Pack in which the task will be saved. Note that if the monitor you are creating the task for resides in an unsealed Management Pack, this Management Pack must be selected here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| General                            | On the General page, you specify a meaningful name for the diagnostic task and optionally provide a description. This can be useful when you need to provide additional details about the task, including how the task is used. You also select the health state for which the task will run, such as Warning or Critical. The diagnostic target can also be changed here, but typically this is not changed because the diagnostic target targets the monitor for which the task is being created. Finally, you can choose whether the task should be run automatically or manually.                                                                                                                                                                                                                                                                                                                                                          |
| Command Line                       | Displayed only when the Run Command option is selected on the Diagnostic Task Type page. You specify the full path to the file to be run, such as C:\Windows\System32\ping.exe. You can also include parameters that should be passed to the command. Including the parameters is very useful because the parameters are context-sensitive. For example, if you are creating a diagnostic task for the Cluster Disk – Free Space monitor, you can add parameters such as the Cluster Disk Name or Partition Name. Adding these parameters means that the command being run can be generic and used for a number of different cluster disks without you having to create a task for each. You can also provide the working directory for the command and set, in seconds, the time-out time frame in which the task should complete. The default is 15 seconds. If the task runs for longer than this period, the task is stopped by the agent. |

| Create Diagnostic Task Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Specify Script Details             | Displayed when the Run Script option is clicked on the Diagnostic Task Type page. You specify the file name of the script to run, such as MyScript.vbs or MyScript.js. Scripts created in either Microsoft Visual Basic or Jscript are supported. You then either manually type the script into the Script box or you can paste the contents of a copied script. This is useful as you can use the script editor such as in Visual Basic to create and test the script and then copy the contents into the Script box after you have finished testing it. As with the Command Line option you can also add context sensitive parameters to the script using the Parameters button. You also specify the timeout value in seconds, minutes, hours or days in which the script must complete before it is forcibly stopped by the agent. |

After you create the diagnostic task, the task is displayed in the Diagnostics section of the Diagnostic And Recovery tab in the monitor properties. The task can also edited and removed from here.

When you create a recovery task, the pages of the wizard are configured in exactly the same manner described earlier in this topic. There is, however, one additional option available on the General page of the Create Recovery Task Wizard: the Recalculate Monitor State After Recovery Completes option. This option is very useful when used in conjunction with monitors that run on a schedule basis and have on-demand detection built in. After completing the recovery task, Operations Manager initiates a Recalculate Health on the monitor. If the recovery task was successful, the monitor's health state returns to healthy automatically.

 **Note:** You can use the Get-SCOMDiagnostic and Get-SCOMRecovery PowerShell Cmdlets to retrieve a list of diagnostics or recoveries that have been configured in Operations Manager. The following command retrieves a list of diagnostics that have the word DinnerNow\_Database in their name:

```
Get-SCOMDiagnostic -Name "*DinnerNow_Database*"
```

## Demonstration: Adding a Diagnostic Task to a Monitor

In this demonstration, you will learn how to add, to a monitor in Operations Manager, a diagnostic task that returns the list of processes running on an agent-managed computer.

### Demonstration Steps

- To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Authoring</b>          |
| View     | <b>Monitors</b>           |

- In the **Look for** box search for **health service heartbeat**, and then expand **Health Service Watcher\Entity Health\Availability**, and then edit the **Service Heartbeat Failure** monitor
- From the **Diagnostic And Recovery** tab, create a new diagnostic task for a critical health state by using the following settings (all other settings should remain the default settings):
  - Diagnostic Task Type: **Run Command**
  - Management Pack: Create a new Management Pack named **Health Service Availability Monitor Overrides**
  - Diagnostic name: **Return Process List\_Demo**
  - Deselect **Run diagnostic automatically**
  - Full path to file: **%windir%\system32\tasklist.exe**
- Open the Active Alerts view in the **Monitoring** pane.
- Stop the Microsoft Monitoring Agent Service on LON-DC1.
- Wait for the **Health Service Heartbeat Failure** alert to appear in the Operations console.
- From the alert, open the Operations Manager Health Explorer.
- Select the **Health Service Heartbeat Failure** monitor.
- From the **State Change Events** tab, run the **Return Process List\_Demo** task.
- Review the output from the Return Process List task.
- Start the **Microsoft Monitoring Agent** Service on LON-DC1.

Verify the correctness of the statement by placing a mark in the column to the right.

| Statement                                                                                                                  | Answer |
|----------------------------------------------------------------------------------------------------------------------------|--------|
| When creating diagnostic and recovery tasks you can only enable the Recalculate Monitor State option with a Recovery Task. |        |

# Lab: Customizing the Operations Console

## Scenario

Contoso, Ltd., has a number of support teams that manage specific applications. For example, one support team manages AD DS whereas another support team manages SQL Server.

You have been asked by your IT manager to configure the Operations console for each team so that they can manage their applications and services appropriately.

In addition, you have been asked to configure notification subscriptions for each team and, where applicable, create diagnostic and recovery tasks that can help troubleshoot and remediate issues detected by Operations Manager.

## Objectives

After completing this lab, you will be able to:

- Create user roles.
- Create a custom resolution status.
- Create custom views.
- Configure notification subscriptions.
- Configure diagnostic and recovery tasks.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machines:** 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-AP1, 10964C-LON-AP2

**User Name:** Contoso\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps.

1. On LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Contoso**
5. Repeat steps 2–4 for the following virtual machines:
  - 10964C-LON-SQ1
  - 10964C-LON-MS1 (LON-HOST2)
  - 10964C-LON-AP1
  - 10964C-LON-AP2 (LON-HOST2)



**Note:** Before you start this lab, make sure that all Windows services that are set to start automatically are running. The exceptions are the Microsoft .NET Framework NGEN v4.0.30319\_X86 and the.NET Framework NGEN v4.0.30319\_X64 services, because these services stop automatically when they are not being used.

## Exercise 1: Creating User Roles and importing the Active Directory Management Packs

### Scenario

For each support team to use a scoped Operations console that includes only the views and tasks applicable to them, you must create a user role for each team. You must also create an Active Directory user account named ADAdmin and an Active Directory Group named AD\_Admins. You must then add the ADAdmin user Account to the AD\_Admins group.

The main tasks for this exercise are as follows:

1. Import the Active Directory management packs
2. Create a user role for the SQL Server support team
3. Create a user role for the Active Directory support team
4. Test user role functionality

#### ► Task 1: Import the Active Directory management packs

1. To perform this step, use the computer and tool information in the following table.

| Location          | Value                           |
|-------------------|---------------------------------|
| Computer          | <b>LON-MS1</b>                  |
| Tool              | <b>Operations Manager Shell</b> |
| Folder            | <b>C:\ADMPs</b>                 |
| PowerShell Script | <b>ImportADMPs.ps1</b>          |

2. Using the **Operations Manager Shell** run the **ImportADMPs.ps1** PowerShell script to import the Active Directory Management Packs.

#### ► Task 2: Create a user role for the SQL Server support team

1. To perform this step, use the computer and tool information shown in the following table.

| Location | Value                      |
|----------|----------------------------|
| Computer | <b>LON-MS1</b>             |
| Tool     | <b>Operations Console</b>  |
| Pane     | <b>Administration</b>      |
| View     | <b>Security\User Roles</b> |

2. Use the Create User Role Wizard to create a user role by using the following settings (all other settings should remain the default settings):
  - Profile: **Operator**
  - User role name: **SQL Administrators**
  - User role members: **Contoso\SQL\_Admins**
  - Group Scope: Select all groups that are prefixed with **SQL**
  - Tasks: Add all tasks that belong to Management Packs that begin with **SQL**
  - Dashboards and Views: On the **Monitoring Tree** tab, add the **Microsoft SQL Server** folder, and then ensure all subfolders and views are also added

► **Task 3: Create a user role for the Active Directory support team**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                      |
|----------|----------------------------|
| Computer | <b>LON-MS1</b>             |
| Tool     | <b>Operations Console</b>  |
| Pane     | <b>Administration</b>      |
| View     | <b>Security\User Roles</b> |

2. Use the Create User Role Wizard to create a user role by using the following settings (all other settings should remain the default settings):
  - Profile: **Operator**
  - User role name: **AD Administrators**
  - User role members: **Contoso\AD\_Admins**
3. Group Scope: Add the following groups:
  - **Active Directory Topology Root**
  - **AD Domain Controller Group (Windows 2000 Server)**
  - **AD Domain Controller Group (Windows 2003 Server)**
  - **AD Domain Controller Group (Windows Server 2008 and above)**
  - **AD Monitoring Client Computer Group**
4. Tasks: Add all tasks that belong to Management Packs that begin with **Active Directory**
5. Dashboards and Views: On the **Monitoring Tree** tab, add the **Microsoft Windows Active Directory** folder, and then ensure all subfolders and views are also added.

► **Task 4: Test user role functionality**

1. To perform this step, use the computer and tool information the following table.

| Location | Value                                     |
|----------|-------------------------------------------|
| Computer | <b>LON-MS1</b>                            |
| Tool     | <b>Operations Console</b>                 |
| Pane     | <b>Monitoring</b>                         |
| View     | <b>Microsoft Windows Active Directory</b> |

2. Create a shortcut on the desktop to the Operations console.
3. Use the **Run as different user** option to open the Operations console as **Contoso\adadmin**.
4. Expand **Microsoft Windows Active Directory**, and then open the **DC State** view.
5. Confirm that only **LON-DC1.CONTOSO.COM** is visible in the details pane.
6. Open the **DC Active Alerts** view.
7. Confirm that all alerts displayed relate to AD DS.
8. Close the Operations console.
9. Use the **Run as different user** option to open the Operations console as **Contoso\sqladmin**.
10. Expand **Microsoft SQL Server**, and then open the **Computers** view.
11. Confirm only **LON-API1.CONTOSO.COM**, **LON-AP2.CONTOSO.COM**, **LON-SQ1.CONTOSO.COM** and **LON-SC1.CONTOSO.COM** are visible in the details pane.
12. Open the **Active Alerts** view.
13. Confirm that any alerts displayed relate to SQL Server.
14. Close the Operations console.

**Results:** After this exercise, you should have created a User Role in Operations Manager for the Active Directory support team and the SQL Server support team. You should have also confirmed that the Operations console is scoped appropriately by opening the console as a member of each team.

## Exercise 2: Creating Custom Resolution States

### Scenario

For Operations Manager operators to assign alerts to the appropriate support teams, you must create the appropriate alert resolution state. You must create one for the SQL Server support team and one for the Active Directory support team. When SQL Server or Active Directory alerts are generated in the Operations console, they can then be assigned to the appropriate team.

The main tasks for this exercise are as follows:

1. Create an alert resolution state for the SQL team
2. Create an alert resolution state for the Active Directory team
3. Test the alert resolution states

#### ► Task 1: Create an alert resolution state for the SQL team

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Settings\Alerts</b>    |

2. Add a new alert resolution state by using the following settings:

- Resolution state: **SQL Server Support**
- Unique ID: **30**

#### ► Task 2: Create an alert resolution state for the Active Directory team

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Settings\Alerts</b>    |

2. Add a new alert resolution state by using the following settings:

- Resolution state: **Active Directory Support**
- Unique ID: **50**

► **Task 3: Test the alert resolution states**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>Active Alerts</b>      |

2. Set the resolution state for an alert to **SQL Server Support**.
3. Set the resolution state for an alert to **Active Directory Support**.

**Results:** After this exercise, you should have created an alert resolution state for both the SQL Server and Active Directory support teams. You should have also tested the alert resolutions states by assigning alerts to the relevant teams.

## Exercise 3: Creating Custom Views

### Scenario

In addition to the standard Management Pack views created when the SQL and Active Directory Management Packs are installed, you have been asked to create a number of specific views for the Active Directory and SQL Server support teams. These views include an event view that displays specific events relating to Active Directory errors that occur in the Contoso environment. You must also create a Performance view for each team that displays various performance counters for Active Directory and SQL Server.

The main tasks for this exercise are as follows:

1. Create the Management Packs
2. Create Event views
3. Create Performance views
4. Create Alert views
5. Create Diagram views
6. Update the user roles to include the new views
7. Confirm the new views are available in the scoped consoles

#### ► Task 1: Create the Management Packs

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Management Packs</b>   |

2. Create two new Management Packs with the following names:

- **SQL Server Support Team Views**
- **Active Directory Support Team Views**

#### ► Task 2: Create Event views

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |

| Location | Value                                                                              |
|----------|------------------------------------------------------------------------------------|
| View     | <b>SQL Server Support Team Views</b><br><b>Active Directory Support Team Views</b> |

2. Create a new Event view in the **SQL Server Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **SQL Server Events**
  - Show data related to: **SQL DB Engine**
  - Show data contained in a specific group: **SQL Computers**
3. Create a new Event view in the **Active Directory Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **Active Directory Events**
  - Show data related to: **Active Directory DC and Global Catalog Server Role (Windows Server 2008 and above)**
  - Show data contained in a specific group: **AD Domain Controller Group (Windows Server 2008 and above)**

### ► Task 3: Create Performance views

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                                              |
|----------|------------------------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                                     |
| Tool     | <b>Operations Console</b>                                                          |
| Pane     | <b>Monitoring</b>                                                                  |
| View     | <b>SQL Server Support Team Views</b><br><b>Active Directory Support Team Views</b> |

2. Create a new Performance view in the **SQL Server Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **SQL Server Performance**
  - Show data related to: **SQL DB Engine**
  - Show data contained in a specific group: **SQL Computers**
3. Create a new Performance view in the **Active Directory Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **Active Directory Performance**
  - Show data related to: **Active Directory DC and Global Catalog Server Role (Windows Server 2008 and above)**
  - Show data contained in a specific group: **AD Domain Controller Group (Windows Server 2008 and above)**

► **Task 4: Create Alert views**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                                              |
|----------|------------------------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                                     |
| Tool     | <b>Operations Console</b>                                                          |
| Pane     | <b>Monitoring</b>                                                                  |
| View     | <b>SQL Server Support Team Views</b><br><b>Active Directory Support Team Views</b> |

2. Create a new Alert view in the **SQL Server Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **Alerts Assigned to SQL Server Support**
  - Select conditions: **with specific resolution state**
  - Resolution state: **SQL Server Support (30)**
3. Create a new Alert view in the **Active Directory Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **Alerts Assigned to Active Directory Support**
  - Select conditions: **With specific resolution state**
  - Resolution state: **Active Directory Support (50)**

► **Task 5: Create Diagram views**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                                              |
|----------|------------------------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                                     |
| Tool     | <b>Operations Console</b>                                                          |
| Pane     | <b>Monitoring</b>                                                                  |
| View     | <b>SQL Server Support Team Views</b><br><b>Active Directory Support Team Views</b> |

2. Create a new Diagram view in the **SQL Server Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **SQL Server Components**
  - Target: **SQL Components**
  - Template: **Create your own**
  - Levels to Show: **4**

3. Create a new Diagram view in the **Active Directory Support Team Views** folder by using the following settings (all other settings should remain the default settings):
  - Name: **Active Directory Components**
  - Target: **AD Domain Controller Group (Windows Server 2008 and above)**
  - Template: **Create your own**
  - Levels to Show: **4**

► **Task 6: Update the user roles to include the new views**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                      |
|----------|----------------------------|
| Computer | <b>LON-MS1</b>             |
| Tool     | <b>Operations Console</b>  |
| Pane     | <b>Administration</b>      |
| View     | <b>Security\User Roles</b> |

2. Edit the **SQL Administrators** user role, and on the **Dashboards and Views** tab, select the **Microsoft SQL Server** and **SQL Server Support Team Views**, ensuring all subfolders and views are selected.
3. Edit the **AD Administrators** user role, and on the **Dashboards and Views** tab, select the **Microsoft Windows Active Directory** and **Active Directory Support Team Views**, ensuring all subfolders and views are selected.

► **Task 7: Confirm the new views are available in the scoped consoles**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                                                                              |
|----------|------------------------------------------------------------------------------------|
| Computer | <b>LON-MS1</b>                                                                     |
| Tool     | <b>Operations Console</b>                                                          |
| Pane     | <b>Monitoring</b>                                                                  |
| View     | <b>SQL Server Support Team Views</b><br><b>Active Directory Support Team Views</b> |

2. Open the Operations console by using the **Run as different user** option, and log in by using the **Contoso\sqladmin** user name and the password **Pa\$\$w0rd**.
3. Open the Following views:
  - Alerts Assigned to SQL Server Support
  - SQL Server Components
  - SQL Server Events
  - SQL Server Performance

4. Close the Operations console.
5. Open the Operations console using the Run as different user option and login using the Contoso\adadmin user name and Pa\$\$w0rd
6. Open the Following views:
  - Active Directory Components
  - Active Directory Events
  - Active Directory Performance
  - Alerts Assigned to Active Directory Support
7. Close the Operations console.

**Results:** After this exercise, you should have created custom views for both the SQL Server support team and Active Directory support team. These views include Events, Performance Counters, Alerts, and Diagrams for the respective teams.

## Exercise 4: Configuring Notifications

### Scenario

For the Active Directory and SQL Server support teams to receive an email when an alert is generated in Operations Manager, you must configure notification subscriptions. A notification subscription must be configured for each team. This notification subscription notifies the team by email whenever an alert relating to the team's application is generated.

The main tasks for this exercise are as follows:

1. Configure an SMTP notification channel
2. Configure a notification subscriber for the Active Directory and SQL Server support teams
3. Configure a notification subscription for the Active Directory and SQL Server support teams
4. Test notifications

#### ► Task 1: Configure an SMTP notification channel

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                         |
|----------|-------------------------------|
| Computer | <b>LON-MS1</b>                |
| Tool     | <b>Operations Console</b>     |
| Pane     | <b>Administration</b>         |
| View     | <b>Notifications\Channels</b> |

2. Create a new Email (SMTP) notification channel by using the following settings (all other settings should remain the default settings):
  - SMTP Server: **LON-AP1.CONTOSO.COM**
  - Authentication method: **Windows Integrated**

- Return Address: **Administrator@contoso.com**
3. Start the **SMTP Virtual Server** from **Internet Information Services (IIS) 6.0 Manager** on LON-AP1.

► **Task 2: Configure a notification subscriber for the Active Directory and SQL Server support teams**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                            |
|----------|----------------------------------|
| Computer | <b>LON-MS1</b>                   |
| Tool     | <b>Operations Console</b>        |
| Pane     | <b>Administration</b>            |
| View     | <b>Notifications\Subscribers</b> |

2. Create a new subscriber that includes the following settings (all other settings should remain the default settings):

- Subscriber Name\Address Name: **SQLAdmin**
  - Channel: **E-Mail (SMTP)**
  - Delivery address for the selected Channel: **sqladmin@contoso.com**
3. Create a new subscriber that includes the following settings (all other settings should remain the default settings):
- Subscriber Name\Address Name: **ADAdmin**
  - Channel: **E-Mail (SMTP)**
  - Delivery address for the selected Channel: **adadmin@contoso.com**

► **Task 3: Configure a notification subscription for the Active Directory and SQL Server support teams**

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>Active Alerts</b>      |

2. Stop the Microsoft Monitoring Agent on LON-SQ1 and LON-DC1.
3. Wait for the **Health Service Heartbeat Failure** alert on LON-SQ1 to appear, and then from the **Tasks** pane, use the **Create** task to create a **Notification Subscription** for the selected alert by using the following settings (all other settings should remain the default settings):
  - Criteria **with specific resolution state of SQL Server Support**

- Subscribers: **SQLAdmin**
  - Channels: **SMTP Channel**
4. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>Active Alerts</b>      |

5. Wait for the **Health Service Heartbeat Failure** alert on LON-DC1 to appear, and then from the **Tasks** pane, use the **Create** task to create a **Notification Subscription** for the selected alert by using the following settings (all other settings should remain the default settings):
- Criteria **with specific resolution state of Active Directory Support**
  - Subscribers: **ADAdmin**
  - Channels: **SMTP Channel**

#### ► Task 4: Test notifications

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>Active Alerts</b>      |

2. Set the resolution state of the **Health Service Heartbeat Failure** alert on LON-SQ1 to **SQL Server Support**.
3. Confirm the email message is sent to SQLAdmin by viewing the EML file that is located in **\LON-AP1\C\$\InetPub\MailRoot\Drop**.
4. Delete the email message.
5. Set the resolution state of the **Health Service Heartbeat Failure** alert on LON-DC1 to **Active Directory Support**.
6. Confirm the email message is sent to **ADAdmin** by viewing the EML file that is located in **\LON-AP1\C\$\InetPub\MailRoot\Drop**.
7. Delete the email message.
8. Start the **Microsoft Monitoring Agent** Service on LON-SQ1 and LON-DC1.

**Results:** After this exercise, you should have created a notification subscription for both the SQL Server support team and the Active Directory support team. You should have then tested that email notifications were working by generating an alert and confirming the relevant support teams were notified via email.

## Exercise 5: Configuring Diagnostic and Recovery Tasks

### Scenario

The SQL Server support team currently troubleshoots issues by using a manual procedure. You have been asked if some of these procedures can be automated by using a diagnostic task in Operations Manager. In addition, the team has supplied a script that they use to remediate common issues that occur in their environment. You must add this script to a recovery task to enable automatic remediation in Operations Manager.

The main tasks for this exercise are as follows:

1. Create a recovery script
2. Create diagnostic and recovery tasks
3. Test diagnostic and recovery tasks

#### ► Task 1: Create a recovery script

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                      |
|----------|----------------------------|
| Computer | <b>LON-SQ1</b>             |
| Tool     | <b>Windows Explorer</b>    |
| Folder   | <b>C</b>                   |
| File     | <b>RestartSQLAgent.bat</b> |

2. Create a file named **RestartSQLAgent.bat** in the C on LON-SQ1 and add the following text to the file:

```
Net Start SQLSERVERAGENT
```

3. Save the file and then close it.
4. Open **Windows Services** and stop the **SQL Server Agent (MSSQLSERVER)** service.
5. Logoff LON-SQ1.

#### ► Task 2: Create diagnostic and recovery tasks

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations console</b> |

| Location | Value                |
|----------|----------------------|
| Pane     | <b>Monitoring</b>    |
| View     | <b>Active Alerts</b> |

2. In the Operations console, from the **SQL Server Agent Windows Stopped** alert, open the Monitor properties.
3. On the **Diagnostic and Recovery** tab, create a new diagnostic task for a critical health state by using the following settings (all other settings should remain the default settings):
  - Diagnostic Task Type: **Run Command**
  - Management Pack: Create a new Management Pack named **SQL Agent Monitor Overrides**
  - Name: **Return Process List**
  - Clear **Run diagnostic automatically**
  - Full path to file: **%windir%\system32\tasklist.exe**
4. On the **Diagnostic and Recovery** tab, create a new recovery task for a critical health state by using the following settings (all other settings should remain the default settings):
  - Diagnostic Task Type: **Run Command**
  - Management Pack: **SQL Agent Monitor Overrides**
  - Name: **Restart SQL Agent**
  - Clear **Run recovery automatically**
  - Full path to file: **C:\RestartSQLAgent.bat**
5. On LON-SQ1, start the **SQL Server Agent (MSSQLSERVER)** service.

#### ► Task 3: Test diagnostic and recovery tasks

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Monitoring</b>         |
| View     | <b>Active Alerts</b>      |

2. On LON-SQ1, stop the SQL Server Agent (MSSQLSERVER) service.
3. In the Operations console, from the **SQL Server Agent Windows Stopped** alert, open the **Health Explorer**.
4. Select the monitor, and then from the **State Change Events** tab, run the following tasks, reviewing the output from each:
  - Return Process List
  - Restart SQL Agent

5. Confirm the SQL Server Agent (MSSQLSERVER) service has been automatically restarted on LON-SQ1.

**Results:** After this exercise, you should have created a diagnostic and recovery task in Operations Manager. You should also have tested the diagnostic and recovery tasks in the Operations console.

**Question:** You have to configure notifications so that an email notification is sent only during work hours. How do you configure this when you create the notification subscriber?

**Question:** You have created a new folder in a monitoring view that is used in a scoped Operations console. When users open their scope in the Operations console, the new folder is not displayed. What do you need to do to ensure the new folder is visible?

# Module Review and Takeaways

## Review Question(s)

**Question:** Explain the difference between diagnostic and recovery tasks.

## Real-world Issues and Scenarios

Before you configure a notification subscription in Operations Manager, you must carefully consider the alerts for which notification is required. Additionally, you should configure the criteria in the subscription so that notifications are sent only when they are required. If, for example, you do not add any criteria to a subscription, notifications will be sent for all alerts.



# Module 9

## Management Pack Authoring

### Contents:

|                                                                                      |      |
|--------------------------------------------------------------------------------------|------|
| Module Overview                                                                      | 9-1  |
| Lesson 1: Management Pack Authoring Concepts                                         | 9-2  |
| Lesson 2: Authoring Management Packs by Using the Operations Console                 | 9-9  |
| Lesson 3: Authoring Management Packs by using the Visual Studio Authoring Extensions | 9-19 |
| Lab: Authoring Management Packs                                                      | 9-35 |
| Module Review and Takeaways                                                          | 9-61 |

## Module Overview

For common applications such as Microsoft SQL Server and Microsoft Exchange Server, a fully developed Management Pack is already available. You can extend the default monitoring contained in Microsoft System Center 2012 R2 Operations Manager by creating rules, monitors, and groups within the Operators console.

However, you might need to author a completely new Management Pack to monitor custom applications. To achieve this, you would author the Management Pack in Microsoft Visual Studio, seal the Management Pack, and then deploy it. The Management Pack should then automatically discover and monitor the components of the application.

Management Pack authoring is a detailed topic that requires a base understanding of the core concepts before proceeding to the authoring process. This module will cover these concepts, including how you create a Management Pack in both the Operations console and Visual Studio.

### Objectives

After completing this module, students will be able to:

- Describe Management Pack authoring concepts.
- Author a Management Pack by using the Operations console.
- Author a Management Pack by using Visual Studio Authoring Extensions.

# Lesson 1

## Management Pack Authoring Concepts

At a conceptual level, it is important that you understand the key components of a Management Pack before you embark on building your own. This lesson covers the fundamentals, from defining the application structure through discovering these components and monitoring them.

### Lesson Objectives

After completing this lesson, students will be able to:

- Use classes and relationships.
- Configure discoveries in a Management Pack.
- Configure modules and workflows in a Management Pack.

### Classes and Relationships

Before you understand what a class is in Operations Manager, you should first understand what an object is. An *object* in Operations Manager is considered the basic unit of management and can be represented by a number of elements in the monitored environment, such as a logical disk, a computer, or a SQL Server database. You can think of an object as being an instance of a specific class.

A *class* can be thought of, then, as a specific type of object. For example, consider the Windows Server 2012 Logical Disk class. This class represents all Windows Server 2012 logical disks and can be viewed in the Operations console by using the Discovered Inventory view in the Monitoring pane. To view the objects relating to the Windows Server 2012 Logical Disk class, perform the following steps:

1. In the Operations console, click the **Monitoring** pane, and then click **Discovered Inventory**.
2. From the **Tasks** pane, click **Change Target Type**.
3. In the **Select Items to Target** window that opens, in the **Look for** box, type **logical disk**.
4. Under **Target**, click **Windows Server 2012 Logical Disks**, and then click **OK**.

The Discovered Inventory view updates to show all discovered Windows Server 2012 logical disks. In this scenario, the objects are the logical disks that have been discovered, and the class is Windows Server 2012 Logical Disk.

This scenario should help you understand why targeting is important in Operations Manager when creating rules and monitors. If you targeted a monitor or rule at the Windows Server 2012 Logical Disk class, the monitor or rule would be run on every Windows Server 2012 logical disk.

**A class is a specific type of object, such as the Windows Server 2012 Logical Disk class**

**A class can be of one of the following types:**

- Concrete
- Abstract
- Singleton

Each class must belong to a base class. An example of a base class is the Windows Server Operating System Management Pack. The following illustrates how classes in this Management Pack are defined:

```
Entity
 L Logical Entity
 L Logical Hardware
 L Logical Device
 L Logical Disk
 L Logical Disk (Server)
 L Windows Server 2003 Logical Disk
 L Windows Server 2008 Logical Disk
 L Windows Server 2012 Logical Disk
```

Notice the inheritance of each class. For example, the Windows Server 2003 Logical Disk, Windows Server 2008 Logical Disk, and Windows Server 2012 Logical Disk classes are all based on the Logical Disk (Server) class. Similarly, the Logical Disk (Server) class is based on the Logical Disk class, and so on through to the Entity class. Entity is known as the root class and is the only class that does not have a base class.

### **Class Types**

Three types of classes can be defined in a Management Pack and are described in the following list:

- Concrete classes

*Concrete classes* are classes that identify instances as part of a discovery process. This is the case with most classes in a Management Pack.

- Abstract classes

*Abstract classes* do not identify instances. They are used by other classes as base classes. In the preceding illustration, all of the classes above the Windows Server 2003 Logical Disk, Windows Server 2008 Logical Disk, and Windows Server 2012 Logical Disk classes are abstract classes.

- Singleton Classes

When there is only one instance of a class such as with a distributed application or a group, a *singleton class* is used. In contrast to an instance being discovered by a Management Pack, the instance in a singleton class is created when the Management Pack is imported.

### **Class Relationships**

To associate instances from one class with instances of a different class, a *class relationship* is used. There are two class relationships that can be defined: a hosting relationship and a containment relationship.

#### ***Hosting Relationship***

A class that is hosted by another class is called a *hosted class*, for example, the Logical Disk class, which is hosted by the Windows Computer class. It is important to know whether a class is a hosted class, because if a computer running Windows is removed from Operations Manager, any logical disk instances associated with the class are removed. If this were not the case, over time the Operations Manager database would fill with objects that are no longer monitored, wasting valuable space.

#### ***Containment Relationship***

*Containment relationships* are less restrictive than hosting relationships in that classes can be related but one class does not depend on another class. A containment relationship can be used for controlling health rollup for a monitor. For example, when one object depends on the health of a different object, but they both do not share a hosting relationship, a containment relationship is used. Containment relationships can also be used with groups. For example, objects can be included in a group by using a containment relationship.

## How Discoveries Work

The purpose of discoveries in Operations Manager is to create instances of classes that are defined in a Management Pack—for example, a SQL Server database instance or a computer running Windows Server 2012. Discoveries work in that same way as monitors or rules in that they are downloaded to agent-managed computers and then run locally on the computer being managed. It is the discovery's job to determine whether an application or component, as defined in the respective Management Pack, is installed on the computer and, if so, how many instances of that application are installed. This information is then used by Operations Manager to create the relevant objects in Operations Manager so that those objects can be monitored. Although you cannot create discoveries in the Operations console, you can view and override them in the Object Discoveries view in the Authoring pane. For example, you might want to override the Cluster Disks Discovery and change the discovery interval so that the discovery runs every 12 hours instead of every 24 hours.

**Discoveries in Operations Manager can use one of the following discovery types:**

- Registry
- WMI
- Script (VB or Windows PowerShell)

**Components of a discovery include:**

- Discovered class
- Target
- Frequency
- Data source

### Components of a Discovery

Each discovery has four key components:

- **Discovered class.** This determines the class or classes discovered by the discovery. In most cases, only one class will be discovered by a discovery, but in some cases where a script is used, multiple classes can be discovered by using a single discovery.
- **Target.** The *target* determines where the discovery will run. In many cases, the discovery will not be required to run on every agent-managed computer, so to minimize the load on agent-managed computers, you can configure the target to target only the computers that you know host the application to be discovered.
- **Frequency.** The *frequency* determines how often the discovery will run. Again, to minimize the load on agent-managed computers, the discovery frequency should be configured appropriately.
- **Data source.** The *data source* determines where the discovery should look and the logic it should use to determine if the application is installed on the agent-managed computer.

### Discovery Mechanisms

There are three key mechanisms that discoveries can use:

- **Registry.** The *registry mechanism* detects the existence of a registry key or data within a registry value. Most applications store details about the application in the registry, so this is typically the preferred discovery mechanism to use. This is the most efficient of all discovery mechanisms and is typically used when a discovery is targeted at the All Windows Computers class, because the mechanism requires the least amount of overhead.
- **Windows Management Instrumentation (WMI).** The *WMI mechanism* can be used to discover any information that is contained within WMI, such as a Windows Service or information contained within the BIOS of a computer.
- **Script.** When neither the registry nor WMI discovery mechanisms can be used, a VB or Windows PowerShell script can be used to discover the application. Using a script provides the ability to build more complex logic into the discovery and allows for multiple classes to be discovered from within a single script. Although scripts provide the most flexibility when performing a discovery, they also consume the most resources on the agent-managed computer. For this reason, you should use scripted discoveries only when necessary.

## The Discovery Process

To understand how discoveries work in Operations Manager, review the following description of the discovery process:

1. The discovery is run on the agent-managed computer.
2. If the discovery detects the application, the discovery gathers information about its instances and properties.
3. If there are any changes to a previously discovered instance, or the instance has been discovered for the first time, this discovery data is sent to a Management Server so that its integrity can be checked.
4. The discovery data is verified by the Management Server for validity against elements such as the class and properties of the discovered instance. If any invalid data is discovered at this stage, the discovery process stops.
5. If the data is valid, the data is then inserted into the Operations Manager database, where one of three additional processes occurs:
  - If the object discovered is new, a new instance is created in the database.
  - If the object already exists, a check is performed to determine whether any properties have changed and, if so, the updates are applied to the same object in the database.
  - If the object already exists but is no longer part of the discovery data, the object is removed from the database. That is, if the discovery previously discovered an object and then subsequently the same discovery no longer discovers it, the object is removed.
6. After the object has been inserted into the database, the object becomes available in Operations Manager and can be monitored in the same way as any other object.

## Modules and Workflows

Modules and workflows in Operations Manager work very closely together. A *workflow* can be thought of as a process run by the Operations Manager agent on an agent-managed computer. A typical workflow would be a rule, monitor, or discovery. The Operations Manager agent loads workflows as defined in Management Packs for the applications being monitored, and then runs them on the agent-managed computer. A workflow contains one or more modules that are used to perform specific functions such as running a script, checking an event, or collecting performance counters. By combining different modules, a workflow can be used to perform complex monitoring in almost any scenario. The following sections provide a detailed description of modules and workflows.

### Module types in a Management Pack include:

- Data source modules
- Probe action modules
- Condition detection modules
- Write action modules

### Workflow types in a Management Pack include:

- Discoveries
- Rules
- Tasks
- Monitors
- Diagnostics
- Recoveries

## Modules

To help you understand what modules do, you can examine the properties of a module included with the Microsoft Windows Library Management Pack. Included in this Management Pack is a module named Microsoft.Windows.TimedScript.PropertyBagProvider, which is used to run a specific script and generate results into a *property bag*. As with most modules, this particular module requires parameters to run. In the case of the Microsoft.Windows.TimedScript.PropertyBagProvider module, the following parameters are required:

- **IntervalSeconds.** How often the script will run
- **SyncTime.** The synchronization time for the script
- **ScriptName.** The script name
- **ScriptBody.** The script body
- **Arguments.** The command-line arguments for the script
- **TimeOutSeconds.** The number of seconds the scripts run before being forced to stop

Parameters passed to a module can be mandatory or optional. In the preceding list of parameters, for example, the SyncTime and Arguments parameters are optional.

When a module is run, data that it collects is made available in a *data stream*. The data stream is created at module run-time and is used to pass collected data onto the next module in a workflow. Data stream modules can share information within a workflow. When data is passed between modules in a workflow, the data must be presented to the workflow by using an expected data type. In the case of the Microsoft.Windows.TimedScript.PropertyBagProvider module, the data type is property bag. If, for example, the next module in the workflow expects a different data type, such as a performance counter data type, an additional module can be added to the workflow to map the data between the two different data types.

### **Module Types**

There are four different types of modules that can be used within a Management Pack. A description of each module type is included in the sections that follow.

#### **Data Source Modules**

*Data source modules* are used at the beginning of a workflow and thus do not require any input. Data source modules are used to collect data such as event log data in an event collection rule. This data is then passed to the data stream in a workflow for use by the next module. A typical data source module would be the Microsoft.Windows.EventProvider module included in the Microsoft.Windows.Library Management Pack. This module collects events based on specified criteria from the Windows Event Log, such as a SQL Server error event, and makes this information available in the data stream.

#### **Probe Action Modules**

*Probe action modules* are similar to data source modules in that they are used to collect data and make it available in the data stream for another module to work with; however, they require a trigger to run. For this reason, probe action modules are typically used with monitors to detect a given condition, or are used with diagnostic and recovery tasks that run after a condition has been detected. Only when a given condition is detected is the probe action module run. A typical probe action module would be the Microsoft.Windows.WmiProbe module included in the Microsoft.Windows.Library Management Pack. This module runs a WMI query to retrieve information from WMI, such as the status of a Windows service.

#### **Condition Detection Modules**

*Condition detection modules* are different from data source and probe action modules in that they can work with more than one input stream of data. They are typically used with rules and monitors and perform one of these three functions:

- **Filter input data.** The condition detection module can be used to detect whether a performance counter exceeded a given threshold or an event in the event log meets given criteria.
- **Map data.** The condition detection module can be used to map data that is retrieved from a script in a data source module to performance data so that it can be inserted into the Operations Manager database.
- **Consolidate data.** The condition detection module can be used to determine when a number of events of the same type have occurred, such as those generated during an intrusion attempt.

A typical condition detection module would be the System.ExpressionFilter module that is included in the System.Library Management Pack. This module evaluates data presented to it from a previous module and then, based on criteria, determines whether data should be passed onto the next module in the workflow.

### **Write Action Modules**

*Write action modules* are typically used at the end of a workflow because they have no output. Rather, they make a change in the environment such as generating an alert or running a script. Write action modules are also used to write data to the Operations Manager database. A change could be made within Operations Manager itself or to the agent-managed computer on which the workflow is running. A typical write action module would be the System.Health.GenerateAlert module included in the System.Health.Library Management Pack. This module is used to generate an alert in Operations Manager.

### **Workflows**

As mentioned earlier, a workflow contains one or more modules. In the earlier example used, in which the Microsoft.Windows.TimedScript.PropertyBagProvider module is used to collect data from a script, this module could be combined, in a workflow, with two other modules that are used to map the collected data to a performance data type and then save the performance data to the Operations Manager database. To perform these functions, the three modules described in the following table would be included in the workflow.

| Timed Script                                                                                                                     | Performance Mapper                                                                                                                                                                                                                                                                                                                                 | Publish Performance Data                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| This module (as described earlier) runs a script that collects data and generates the output to a property bag on a timed basis. | This module maps the data provided in the property bag to the performance data type. Required parameters, such as the ObjectName, CounterName, InstanceName, and Value, can be obtained either from the data in the property bag or from static values and/or variables such as the \$Target variable, which can be used to identify the instance. | This module accepts the performance data from the data stream and then publishes it to the Operations Manager database. |

As with monitors and rules, workflows require a target to determine on which agents they should run. This includes how many copies of the workflow will be run, because a separate workflow is required for each instance of the targeted class. For each workflow that runs, that workflow's data stream and property values are treated as separate entities. This is important to understand: for example, explicit values can be common across all workflows, whereas variables such as the \$Target variables can be used to resolve different values, depending on the instance that the workflow is running against.

### **Workflow Types**

Six workflow types that can be included in a Management Pack:

- **Discoveries.** *Discoveries* use a single data source module, which generates discovery data for insertion into the Operations Manager database.
- **Rules.** *Rules* can be used to collect data, generate alerts, and run a script on a scheduled basis. They can be used with multiple data source modules and incorporate a condition detection module. Multiple write action modules can also be included with this workflow type.
- **Tasks.** *Tasks* can use either a probe action module or a write action module depending on the task being run. For example, a probe action module could be used to collect information relating to the processes running on an agent-managed computer.
- **Monitors.** *Monitor* workflows can use either a regular detection (most common) type, where the monitor is constantly checking the monitored object, or an on-demand detection, where the

monitored object is checked when it is brought out of maintenance mode, or a Reset Health action is performed against it.

- **Diagnostics.** *Diagnostic* workflows use a condition detection module and a probe action module. For example, the condition detection module can be used to check the health state of a given object, and the probe action module can be used to collect data about the object when the health state changes to critical.
- **Recoveries.** Similar to a diagnostic workflow, the *recovery* workflow uses a condition detection module to detect a given state of a monitored object. A write action module is also used in a recovery workflow to perform a recovery action. This can be automatically initiated when a given condition is detected, or it can be run manually.

**Question:** What are the four key components of a discovery?

## Lesson 2

# Authoring Management Packs by Using the Operations Console

Authoring a Management Pack can be performed by using a number of different methods: the Operations console, Authoring console, Visio Management Pack Designer, and Visual Studio Authoring Extensions.

For common monitoring scenarios, you can use the Operations console to create a Management Pack. Rules, monitors, and views can then be created and saved in the Management Pack. The Management Packs can be exported and sealed, if necessary, and then imported into other Management Groups, where an override Management Pack can be used to customize the rules and monitors for the new environment.

It is important to understand how to author Management Packs by using the Operations console, because this method will be the most common method adopted when customizing monitoring in your environment.

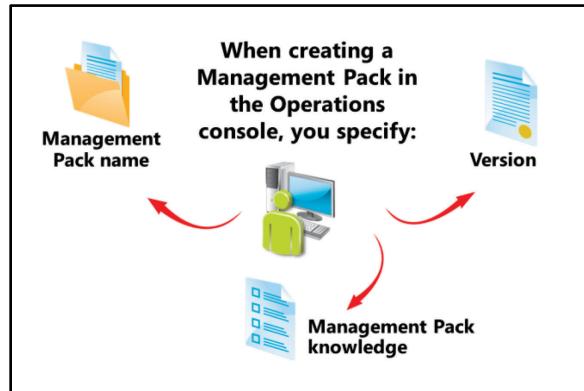
## Lesson Objectives

After completing this lesson, students will be able to:

- Create a Management Pack in the Operations console.
- Add rules to a Management Pack.
- Add monitors to a Management Pack.
- Create groups to target overrides
- Export and seal a Management Pack.

## How a Management Pack Is Created by Using the Operations Console

You can create a Management Pack by using the Create A Management Pack wizard in the Operations console. The Create A Management Pack wizard can be started by clicking the Create Management Pack task from the Tasks pane when the Management Packs node is selected in the Administration pane. The wizard can also be opened by clicking the New button next to the Management Pack drop-down list when performing other actions in the Operations console, such as when creating a rule or monitor.



The following table describes the pages of the Create A Management Pack wizard and the page settings.

| Create A Management Pack wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties                   | Type the name of the Management Pack as it will be displayed in the Operations console. You should provide a descriptive name for the Management Pack, especially if it is a Management Pack that will be used to store overrides for a sealed Management Pack. For example, if creating a Management Pack to store overrides for SQL Server, you should name the Management Pack something similar to SQL Server Management Pack Overrides. This name helps identify Management Packs in the Operations console when you need to export them. As you enter the name of the Management Pack, the Management Pack ID is automatically populated and cannot be changed. This is how the Management Pack will be referenced when viewing the XML code. You can optionally include a description for the Management Pack, which can be useful when you need to describe certain functions that the Management Pack provides or a list of overrides that the Management Pack includes. You also specify the version of the Management Pack. By default, the version is set to 1.0.0.0, but you can specify any dotted number value such as 2.0 or 4.5.6.7. The version can be used to help with Management Pack version control in Operations Manager. As new versions of a Management Pack are created, they can be compared with any earlier versions already imported in Operations Manager to help ensure you have the most up-to-date version installed. |
| Knowledge                            | Add product-specific knowledge that will be saved with the Management Pack. This could include details of the components included in the Management Pack and what the Management Pack's function is. Note that this is different from company knowledge, which can be added to rules and monitors within a Management Pack and is used to help troubleshoot issues detected by the Management Pack.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

After adding any product knowledge for the Management Pack, you click the Create button to create the Management Pack. After the Management Pack is created, it is displayed in the Management Packs node in the Administration pane of the Operations console.

## Add Rules to a Management Pack

You can author rules and monitors in Operations Manager by using the Create A Rule or Create A Monitor task that is available in the Tasks pane when either the Rules or Monitors node is selected in the Management Pack Objects node in the Authoring pane of the Operations console. When creating a rule, the Create Rule Wizard is used to configure the settings for the rule. In the following table, the pages of the Create Rule Wizard are described, including the settings configured on each page. In the table, the following scenario is used to discuss the settings of the wizard: an NT Event Log (Alert) rule is being created, which will be used to generate an alert when event ID 1102 is detected on a computer running Windows Server 2012, denoting that the Security event log has been cleared.

**When creating an NT Event Log rule in the Operations console, you use the Create Rule Wizard and include the following:**

- Management Pack where the rule should be saved
- Target of where the rule should be run
- Event details to detect
- Alert priority and severity
- Alert description
- Alert suppression

| Create Rule Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule Type               | Select the type of rule to create, such as an alert generating rule or collection rule. In this scenario, the NT Event Log (Alert) rule is selected from the event-based alert generating rules list. You also select or create an unsealed Management Pack in which the rule will be saved.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| General                 | On the General page you Add a descriptive name for the rule, such as Security Event Log Cleared. You can optionally include a description. You can also select the Rule Category, such as Alert or Event Collection, depending on the type of rule you are creating. You must also select the rule target on this page, which determines to which agents the rule will be distributed. This is an important setting because, for example, if you select All Windows Computers as the target, the rule will be distributed to any computer that is running any Windows operating system. You should target the rule appropriately so that it is distributed only to computers where it should run. In this scenario, the Windows Server 2012 Operating System class is selected. By default when creating the rule, this rule is automatically enabled. You can clear the Rule Is Enabled check box on this page if you do not want the rule to be enabled. This is useful when you need to enable the rule on a group of computers by using an override, for example. |
| Event Log Type          | Select the event log that should be searched. Event logs include Application, Hardware Events, Operations Manager, Security, System, and Windows PowerShell. In this scenario, the Security event log is selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Build Event Expression  | Define the criteria that will be used to match the event ID to be detected. You can build criteria based on a number of event properties such as the Event ID, Event Source, User, and Event Category. You can also include specific parameters of an event, which is useful when there are key values to be detected in an event. In this scenario, an Event ID parameter is added with an Equals operator and a value of 1102. An Event Source parameter is also added with an Equals operator and a value of Eventlog.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Create Rule Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure Alerts        | Configure the alert priority and alert severity. This is useful for operators when ascertaining which alerts should be worked on first in the Operations console. For example, a service failure alert on a nonbusiness-critical application server might have a severity of critical and a priority of medium, whereas a service failure on a business-critical application server might have a severity of critical and a priority of high. You can also configure the alert description on this page and include context-sensitive parameters such as DNS Name or IP Address. This is useful when you need to add detailed information that should be included in the alert description to assist the operator in resolving the alert. You can also configure alert suppression on this page. This is useful in minimizing the number of alerts generated in the console. For example, by selecting the Logging Computer field, an alert will be generated only once if the computer that logged the event is the same. Instead of multiple alerts for the same computer being generated and filling the Operations console, one alert is generated and the alerts Repeat Count setting is updated each time the event is detected. Other alert suppression fields that can be used include Event Source, Event ID, Event Category, and User. |

After the rule is created, it is immediately evaluated and downloaded by agents that meet the target criteria configured for the rule.

## How Monitors Are Added to a Management Pack

To create a monitor in Operations Manager, you click the Create A Monitor task that is available in the Tasks pane when the Monitors node is selected in the Management Pack Objects node in the Authoring pane of the Operations console. You then select the monitor type such as Unit Monitor, Dependency Rollup Monitor, or Aggregate Rollup Monitor, after which the Create An X Monitor wizard opens (where X represents the monitor type selected, such as Create A Unit Monitor). In this wizard, you complete the settings for the new monitor.

**When creating a Double Threshold performance counter monitor in the Operations console, you use the Create a Monitor Wizard and include:**

- Management Pack where the rule should be saved
- Target of where the rule should be run
- Performance counter to monitor
- Threshold range
- Health states
- Alert priority and severity
- Alert description

Described in the following table are the pages of the Create A Unit Monitor wizard, including the settings configured when using the wizard to create a Double Threshold Windows Performance Counters monitor that detects when CPU utilization is high.

| Create a unit monitor wizard page | Description                                                                                                                                                                                                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitor Type                      | Select the type of monitor to create, such as an Event Reset monitor or a Base Service Monitor. In this scenario, the Double Threshold Windows Performance Counter monitor is selected. You also select or create an unsealed Management Pack in which the monitor will be saved. |
| General                           | Provide a meaningful name, such as CPU Utilization High, and an optional description for the monitor. You also select the Monitor target                                                                                                                                          |

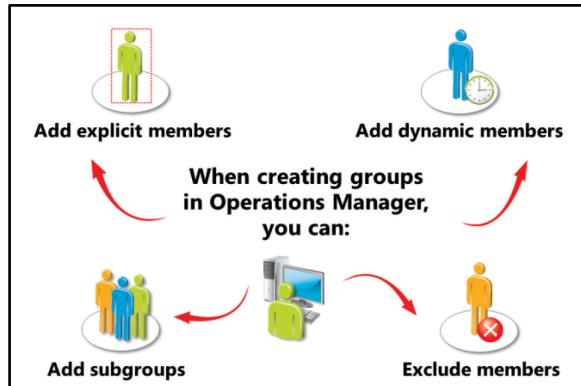
| Create a unit monitor wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | such as Windows Server 2012 Operating System. The target determines on which computers the rule will be downloaded and executed. You must also select the Parent monitor on this page, which determines how the health of the monitor is rolled up in Operations Manager. Parent monitors that can be selected are Availability, Configuration, Performance, and Security. In this scenario, as a performance monitor is being created, the Performance parent monitor is selected.                                                                                                                                                                                                                                                                                                                                                             |
| Performance Counter               | Specify the Object, Counter, and Instance of the performance counter you want to monitor. You can click the Select button, and then either browse to select a local performance counter or connect to a remote computer and select a performance counter. This is useful because you do not need to know the full object, counter, and instance name. Instead, you can simply select the counter from a list, and these values are populated automatically. In this scenario, the % Processor Time counter is selected. You can also opt to include all instances of the selected monitor. This is useful if you need to monitor multiple instances of a counter, such as with multiple CPUs. You also specify the monitoring interval; by default, this is 15 minutes, but you can configure the interval in Seconds, Minutes, Hours, or Days. |
| Threshold Range                   | Specify the Low and High value thresholds. In this scenario, this is a percentage value. For example, to set the low threshold to 70 percent, the value would be specified as 70.00. Similarly to set a high value of 90 percent, the value would be specified as 90.00. These values are key in depicting the health of the monitor being created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Configure Health                  | Map the possible monitor conditions to health states. For example, if the CPU utilization is under 70 percent, the health state of the monitor would potentially be in a warning health state. If the CPU utilization is over 90 percent, the monitor would in a critical health state. If the CPU utilization is between 70 percent and 90 percent, the monitor could be considered as being in a warning state. For each monitor condition, you configure the health state, such as Warning, Critical, or Healthy.                                                                                                                                                                                                                                                                                                                            |
| Configure Alerts                  | Optionally enable alerting for the monitor. By default, this option is not enabled. By selecting the Generate Alerts For This Monitor To Enable Alerting check box, you can then configure the conditions for when an alert should be generated. Options are:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Create a unit monitor wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <ul style="list-style-type: none"> <li>The monitor is in a critical or warning health state.</li> <li>The monitor is in a critical health state.</li> </ul> <p>You can configure the alert priority and severity, and the alert description, as described in the Topic titled "How Rules Are Added to a Management Pack." You can also select the Automatically Resolve The Alert When The Monitor Returns To A Healthy State check box to ensure that only alerts for which the health state remains in a critical or warning state are displayed in the console.</p> |

After the monitor is created, it is evaluated and then downloaded and executed on the computers that match the target as specified on the General page of the Create A Unit Monitor wizard.

## Create Groups to target Overrides

Groups provide a method of grouping objects discovered by Operations Manager. You can then use a configured group to scope alert notifications, reports, and views that are made available in user roles. You can also use groups when configuring overrides. This is useful when you need to enable or disable a monitor or rule for a specific computer. For example, you can create a group that includes a specific computer or computers, such as all Domain Controller computers. You can then create a monitor targeted at All Windows Computers but leave the monitor in a disabled state. Then, using an override, you can enable the monitor for the group containing the DinnerNow computers. The monitor will run only on these computers. You can target any object in Operations Manager in this way.



To create a group in Operations Manager, you use the Create A New Group task, which is available when the Groups node is selected in the Authoring pane of the Operations console. When you use this task, the Create Group Wizard starts, in which you define the group properties. In the following table, each page of the Create Group Wizard is described, including the settings that are configured on each page.

| Create Group Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Properties       | Specify a descriptive name for the group being created, such as All Domain Controllers. You can optionally add a description for the group. You must also select or create an unsealed Management Pack in which the group will be saved.                                                                                                                                                             |
| Explicit Members         | Use the Add/Remove Objects button to add explicit members of the group. This opens an Object Selection window, where you can browse by object type and then select the objects to be included. For example, you can select the Windows Computer object type and then click the Search button to return a list of discovered Windows Computers. You then add the computers you want to include in the |

| Create Group Wizard page | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | group to the Select Objects section.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Dynamic Members          | <p>Use the Create/Edit rules button to create a formula that will be used to dynamically add objects to the group. Doing this is useful because you can create a group that includes all SQL Server databases. Then, when new computers running SQL Server are added to the monitored environment, their databases will automatically be included in this group. As you build the formula, you add combinations of Property, Operator, and Values that together are used as filters to return the object required in the group. For example, you can add the SQL Database object type and configure the Property, Operator, and Value as follows:</p> <ul style="list-style-type: none"> <li>• <b>Property.</b> Database Name</li> <li>• <b>Operator.</b> Contains</li> <li>• <b>Value.</b> Operations</li> </ul> <p>Using this combination of values, any SQL Server database that has the word Operations in its name will be included in the group. As you add each combination of values, you can configure the values to use an AND or OR expression. This makes targeting specific objects very granular.</p> |
| Subgroups                | Use the Add/Remove Subgroups button to add or remove subgroups that should be included or removed from the group being created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Excluded Members         | Use the Exclude Objects button to select objects that should not be included in the group. This is useful when you have used the Dynamic Members page to include a dynamic list of objects. There could be specific objects that the formula returns that you do not want to be included in the group. In this scenario, you would add them to the Excluded Members page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

After configuring the group settings, you click the Create button to create the group. The group is then displayed in the Groups node in the Authoring pane. You can right-click any group in this view and then click View Group Members. This is useful when you need to determine which objects are included in a group before you include the group in a user role or override, for example, and is especially useful when used with groups that use dynamic membership rules.

## The Process of Exporting and Sealing a Management Pack

After you have create a Management Pack and include the Management Pack elements such as rules, monitors, groups, and views, you can export and back up the Management Pack so that it can be restored in the event of a disaster. By exporting the Management Pack, you also make it available to other Operations Manager Management Groups. To protect the Management Pack so that it cannot be changed, you should also seal it. Sealing it ensures that any changes to the Management Pack are configured in a separate Management Pack, thereby protecting the original

You can export **unsealed** Management Packs by using the Export Management Pack task in the Operations console

You can export **sealed** and **unsealed** Management Packs by using the Operations Manager Shell

**To seal a Management Pack, you must first obtain:**

1. The unsealed version of the Management Pack
2. A strong name key file
3. Any referenced Management Packs

content. Sealing a Management Pack also enables elements within it to be referenced by other Management Packs.

### To Export a Management Pack in the Operations Console

To export a Management Pack by using the Operations console, perform the following steps:

1. From the **Administration** pane, click **Management Packs**.
2. From the details pane, click the Management Pack you want to export.
3. From the **Tasks** pane, click **Export Management Pack**.
4. In the **Browse For Folder** window that opens, browse to the folder where you want the exported Management Pack to be saved, and then click **OK**.

The unsealed Management Pack is saved to the specified location. Note that only unsealed Management Packs can be exported by using the Operations console. If a sealed Management Pack is selected in the Management Packs node, the Export Management Pack task is not available.

### To Export Management Packs by Using Windows PowerShell

Using the Operations Manager Shell, you can also export both sealed and unsealed Management Packs.

To export a sealed or unsealed Management Pack perform the following steps:

1. Open the Operations Manager Shell.
2. Type the following command, and then press enter.

```
Get-SCOMManagementPack
```

3. From the list of returned Management Packs, note the name of the Management Pack. For example, System.Library.
4. Type the following command, and then press enter.

```
Get-SCOMManagementPack -name <Name_from_step_3> | Export-SCOMManagementPack -path
“<save_path>”
```

To export the System Library Management pack to the C:\Backup folder, enter the following command.

```
Get-SCOMManagementPack -name System.Library | Export-SCOMManagementPack -path
“C:\Backup”
```

### Sealing a Management Pack

To seal an unsealed Management Pack, if it was created in the Operations console, you must first export it to an unsealed .xml file by using the preceding instructions. You must also have access to the following before sealing a Management Pack:

- The .xml version of the Management Pack to be sealed.
- Access to all Management Packs referenced in the Management Pack to be sealed.
- A key file that contains the private and public keys used to validate the identity of the party signing the Management Pack. You can create a key file by using the Strong Name utility SN.exe that is provided with Visual Studio. The following command uses the SN.exe utility from the Visual Studio 2008 Command Prompt window and creates key file named Contoso.snk.

```
sn -k contoso.snk
```

After you have the key file, the unsealed Management Pack, and the location of any referenced Management Packs, you can seal the Management Pack by using the MPSeal.exe utility that is found in

the SupportTools folder on the Operations Manager media. For example, the following command line seals a Management Pack named DinnerNow.xml by using the Contoso.snk key file. The location of referenced Management Packs is C:\MPs.

```
MPSeal.exe DinnerNow.xml /I C:\MPs /KeyFile Contoso.snk /Company "Contoso"
```

After the command completes, a sealed Management Pack file is created in the folder where the MPSeal.exe utility was run. Note that before you import the sealed Management Pack, you should first remove the unsealed Management Pack from Operations Manager.

Before attempting to seal a Management Pack, you can use the MPVerify.exe utility to check the Management Pack and any dependencies. If there are any issues detected with the Management Pack, they will be displayed in the results generated after running the MPVerify.exe utility. The MPVerify.exe utility can be found in the installation folder where the Operations console is installed. This is typically \Program Files\Microsoft System Center 2012\Operations Manager\Console. The following example command line shows the MPVerify.exe utility being used to check the DinnerNow.xml file with the dependent Management Packs location in C:\Mps.

```
MPVerify.exe /I C:\MPs DinnerNow.xml
```

If successful, a message stating "Verification succeeded" is displayed in the results. If there are any problems verifying the Management Pack, such as a dependent Management Pack not being found, a "Could not load Management Pack" message is displayed, including the Management Pack name that could not be loaded. You can then use this information to obtain the relevant Management Packs before running the MPVerify.exe utility again.

## Demonstration: Creating a Management Pack in the Operations Console

In this demonstration, you will learn how to create a new Management Pack in the Operations console and then add a rule to the Management Pack.

### Demonstration Steps

1. To perform this step, use the computer and tool information in the following table.

| Location | Value                     |
|----------|---------------------------|
| Computer | <b>LON-MS1</b>            |
| Tool     | <b>Operations Console</b> |
| Pane     | <b>Administration</b>     |
| View     | <b>Management Packs</b>   |

2. Using the Create Management Pack task, create a new Management Pack named **Demo**.
3. Confirm the **Demo** Management Pack has been created.
4. Confirm the **Demo** folder has been created in the **Monitoring** pane.
5. From the **Authoring** pane, use the **Create a Rule** task to create a new rule with the following settings (all other settings should remain the default settings):
  - Rule Type: From the Alert Generating Rules section, expand **Event Base**, and then select **NT Event Log (Alert)**
  - Management Pack: **Demo**
  - Rule Name: **Demo Rule**
  - Rule Target: **Windows Server 2008 Operating System**
  - Rule is enabled: **False**
  - Event ID: **5084**
  - Event Source: **MSSQL\$SQLEXPRESS**
  - Alert Suppression: **Event ID**

**Question:** You are creating an alert generating rule and need to ensure that the alert generated by the rule does not get generated more than once for each computer. What option should you configure when creating the rule to facilitate this?

## Lesson 3

# Authoring Management Packs by using the Visual Studio Authoring Extensions

After learning the Management Pack authoring concepts, you can move on to authoring a custom Management Pack by using the Visual Studio Authoring Extensions. When designing your Management Pack, it is important to understand how the service model and health model of the application you need to monitor is represented in the Management Pack. In addition, you should understand how to define views and reports in the Management Pack, which determine how the application will be displayed in the Operations console.

## Lesson Objectives

After completing this lesson students will be able to:

- Describe the Visual Studio Authoring Extensions (VSAE).
- Author a Management Pack in VSAE.
- Add a custom module and discovery.
- Add monitors.
- Add rules.
- Add folders and views.

## Overview of Visual Studio Authoring Extensions

The System Center 2012 Visual Studio Authoring Extensions (VSAE) is a component add-on available for both Visual Studio 2012 and Visual Studio 2013 Professional and Ultimate editions. Using the VSAE add-on, you can create Management Packs for both Operations Manager 2007 R2 and System Center 2012 Operations Manager. Important features of VSAE include the following:

- **Management Pack elements.** Create any Management Pack element such as a rule, monitor, or discovery by working directly within the XML of a Management Pack.
- **XML templates.** XML templates for many Management Pack elements are provided, including IntelliSense, to help you author Management Packs without needing detailed knowledge of Management Pack schema.
- **XML fragments.** XML fragments can be created that contain different Management Pack elements, which can then be shared with other Management Packs.
- **Shared authoring.** Multiple authors can work on the same Management Pack project at the same time.

**The Visual Studio Authoring Extensions features include:**

- Management Pack elements
- XML templates
- XML fragments
- Integrated Resource Kit Tool

**Using Visual Studio Authoring Extensions, you can create Management Packs for:**

- Operations Manager 2007 R2
- Operations Manager 2012
- Operations Manager 2012 SP1
- Operations Manager 2012 R2
- Service Manager 2012
- Service Manager 2012 SP1
- Service Manager 2012 R2

- **Integrated resource kit tools.** Resource kit tools such as Workflow Simulator, Generate Visio Diagram, MP Best Practice Analyzer, MP Spell Checker, and MP Cookdown Analyzer are integrated into VSAE.

To download VSAE, go to the following link:

 **System Center 2012 Visual Studio Authoring Extensions**

<http://go.microsoft.com/fwlink/?LinkId=391277>

### **Installing VSAE and selecting a Management Pack template**

After downloading VSAE, you install it on the computer that is running either Visual Studio 2012 or Visual Studio 2013. Note that Visual Studio must be closed before installing VSAE. When you open Visual Studio after installing VSAE, and you create a new project, a new template named Management Pack becomes available. Seven new Management Pack templates are available:

- **Operations Manager 2007 R2 Management Pack.** Compatible with Operations Manager 2007 R2, Operations Manager 2012, Operations Manager 2012 Service Pack 1 (SP1), and Operations Manager 2012 R2.
- **Operations Manager 2012 Management Pack.** Compatible with Operations Manager 2012, Operations Manager 2012 SP1, and Operations Manager 2012 R2.
- **Operations Manager 2012 R2 Management Pack.** Compatible with Operations Manager 2012 R2.
- **Operations Manager 2012 SP1 Management Pack.** Compatible with Operations Manager 2012 SP1 and Operations Manager 2012 R2.
- **Service Manager 2012 Management Pack.** Compatible with Service Manager 2012, Service Manager 2012 SP1, and Service Manager 2012 R2.
- **Service Manager 2012 R2 Management Pack.** Compatible with Service Manager 2012 R2.
- **Service Manager 2012 SP1 Management Pack.** Compatible with Service Manager 2012 SP1 and Service Manager 2012 R2.

 **Note:** To use the full functionality provided by System Center 2012 R2 Management Packs, such as multi-targeted dashboards, binary development, and new network monitoring modules, you must use the Operations Manager 2012 R2 Management Pack.

### **Using Solution Explorer to Configure a Management Pack**

After you select the appropriate Management Pack template, you can start to configure the Management Pack by using Solution Explorer. Depending on the complexity of the Management Pack you are creating, you might find it easier to organize Management Pack elements such as classes, discoveries, monitors, and rules into separate folders in Visual Studio. You can create a folder in Visual Studio by right-clicking the solution name, clicking Add, and then New Folder. By creating a folder to store your Management Pack elements, you make the Management Pack easier to understand by other authors who might also be working on the Management Pack.

To start working with the Management Pack and adding elements such as rules and monitors, you right-click on either the solution name or a folder within the solution, click Add, and then New Item. This opens the Add New Item dialog box, where you select the item to add to the Management Pack. Items are grouped into five categories as follows:

- Code
- Resources

- Samples
- Templates
- XML

The items in each of these categories are described in the sections that follow.

### **Code**

The code group contains the following three items:

- **Empty Management Pack Fragment.** A Management Pack source file.
- **Empty Management Pack Template Group.** A Management Pack file that allows you to add multiple Management Pack fragment templates such as those described in this section.
- **Snippet Template.** An XML snippet template that can be used to replicate XML data within a Management Pack.

### **Resources**

The resources group contains the following four items:

- **Bitmap File.** Adds a bitmap to the Management Pack, where you can edit it by using editing tools like those in Paint.
- **Jscript Files.** Adds a Jscript file to the Management Pack, where you can edit the script body.
- **PowerShell script file.** Adds a Windows PowerShell script file to the Management Pack where you can edit the script body.
- **VBScript file.** Adds a Microsoft Visual Basic Scripting Edition (VBScript) file to the Management Pack where you can edit the script body.

### **Samples**

The samples group contains the following two items:

- **Datagrid Dashboard.** A sample dashboard is added to the Management Pack that uses a data grid.
- **Hello World Dashboard.** A sample dashboard is added to the Management Pack that includes a folder and dashboard view.

### **Templates**

The templates group contains the following 14 items:

- **Agent Task (Custom).** Creates a new MP Template Group and then adds an agent task to the group, which can then be configured.
- **Agent Task (PowerShell Script).** Creates a new MP Template Group and then adds an agent task to the group, which can then be configured with a Windows PowerShell script.
- **Agent Task (Windows Script).** Creates a new MP Template Group and then adds an agent task to the group, which can then be configured with a Windows script.
- **Assembly Resource.** Creates a new MP Template Group and then adds an Assembly Resource to the group, which can then be configured
- **Discovery.** Creates a new MP Template Group and then adds a Discovery to the group, which can then be configured with the relevant Data Source.
- **Monitor (Aggregate).** Creates a new MP Template Group and then adds an Aggregate Monitor to the group, which can then be configured with the monitor properties.
- **Monitor (Dependency).** Creates a new MP Template Group and then adds a Dependency Monitor to the group, which can then be configured with the monitor properties.

- **Monitor (Unit)**. Creates a new MP Template Group and then adds a Unit Monitor to the group, which can then be configured with the monitor properties.
- **Rule (Alert)**. Creates a new MP Template Group and then adds an alert generating rule to the group, which can then be configured with the rule properties.
- **Rule (Custom)**. Creates a new MP Template Group and then adds a rule to the group, which can then be configured with custom data sources and write actions.
- **Rule (Event Collection)**. Creates a new MP Template Group and then adds an event collection rule to the group, which can then be configured with the rule properties.
- **Rule (Performance Collection)**. Creates a new MP Template Group and then adds a performance collection rule to the group, which can then be configured with the rule properties.
- **Snippet Data**. Adds a snippet data item that can then be configured with XML data manually or from a comma-separated value (CSV) file.
- **View (Custom)**. Creates a new MP Template Group and then adds a view to the group, which can then be configured with the view properties.

## XML

The XML group contains the following eight items:

- **Class**. Adds a Class XML snippet to the Management Pack, which can then be defined for a specific Operations Manager class.
- **Folder & Folder Item**. Adds a folder XML snippet that will be displayed in the Monitoring pane in the Operations console. A Folder Item XML snippet is also added, which can then be configured to display a view in the Operations console.
- **Group**. Adds a Group XML snippet to the Management Pack, which can then be configured with a base class.
- **Linked Report**. Adds a Linked Report XML snippet to the Management Pack, which is then configured for a specific report in Operations Manager.
- **Monitor Diagnostic**. Adds a Diagnostic XML snippet to the Management Pack, which can then be configured with the relevant monitor and modules for the diagnostic task.
- **Monitor Recovery**. Adds a Recovery XML snippet to the Management Pack, which can then be configured with the relevant monitor and modules for the recovery task.
- **Relationship**. Adds a Relationship XML snippet to the Management Pack, which can then be configured with the relevant source and target.
- **Schema Type**. Adds a Schema XML snippet to the Management Group, which can then be configured with data items and a custom schema.

When selecting items to add to a Management Pack, you also provide a name for the item being added. This is important, because each item is created and saved as a separate file in Visual Studio. It is only when the project is built that a resulting Management Pack is created. For example, suppose you add a class to a Management Pack and provide a name of TargetClass. When the class is added, a new window named TargetClass.mpx is opened in Visual Studio. You can then edit the class to include the XML code and attributes of the class being created in the Management Pack. When you finish editing the class, you can right-click the class window tab and then click Save to save the class, or click Open Containing Folder to browse to the folder where the class is saved. Note that this methodology is used for all items added to a Management Pack.

In most cases, when adding an item to a Management Pack you will need to edit the XML data included with the item and/or edit the properties of the item. For example, when adding a Folder & Folder Item to a Management Pack, the following XML code is automatically added.

```

<ManagementPackFragment SchemaVersion="2.0"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <Presentation>
 <Folders>
 <!-- In this section, you can create more folders. Edit the DisplayString for
this folder
 to change the name the user sees in the console. More information can be
found in
 the Management Pack Development Kit: http://msdn.microsoft.com/en-
us/library/ee533810.aspx -->
 <Folder ID="ManagementPack2.Folder2" Accessibility="Internal"
ParentFolder="SC!Microsoft.SystemCenter.Monitoring.ViewFolder.Root" />
 </Folders>
 <FolderItems>
 <!-- In this section, uncomment and edit the ElementID to reference a View or
Folder
 you've created to place that item into the Folder referenced by the Folder
attribute.
 FolderItems do not need display strings; The referenced ElementID's
DisplayString
 is used and shown to the user. More information can be found in the
Management
 Pack Development Kit: http://msdn.microsoft.com/en-
us/library/ee533579.aspx -->
 <!--
 <FolderItem ID="ManagementPack2.FolderItem1" ElementID=""
Folder="ManagementPack2.Folder2" />
 -->
 </FolderItems>
 </Presentation>
 <LanguagePacks>
 <LanguagePack ID="ENU" IsDefault="true">
 <DisplayStrings>
 <DisplayString ElementID="ManagementPack2.Folder2">
 <Name>Folder2 Folder</Name>
 <Description></Description>
 </DisplayString>
 </DisplayStrings>
 </LanguagePack>
 </LanguagePacks>
</ManagementPackFragment>
```

Notice the comments that have been added between the <!-- and --> tags. There is useful information included here that provides assistance when configuring the item in the Management Pack. In the preceding example above, the line "<FolderItem ID="ManagementPack2.FolderItem1" ElementID="" Folder="ManagementPack2.Folder2" />" should be uncommented and edited to reflect the folder as it should be displayed in the Operations console. It is important to review the comments within each item added to a Management Pack because they contain important information about the item's configuration.

### **Building the Management Pack**

After you complete the Management Pack design, you must build it by using the Build option, which compiles the Management Pack files into a single Management Pack. Before doing this, however you should review the Management Pack properties and make any necessary changes. To view the properties of the Management Pack, you right-click the solution name in Solution Explorer and then click Properties. This opens the properties window where four tabs containing a number of Management Pack settings can be configured, as described in the following table.

| Management Pack properties tab name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management Pack                     | Define properties such as the Management Pack ID, Management Pack Version, Management Pack Friendly Name, and the Default Namespace. These settings are automatically populated when loading a Management Pack template, but they can be edited on this tab if desired. You might, for example, want to increase the Management Pack's version number after applying a number of updates to a Management Pack.                                                                                                                                                                                               |
| Build                               | Configure settings relating to how the Management Pack is built. The Generate Sealed And Signed Management Pack check box (when selected) will enable a sealed version of the Management Pack to be created when it is built. When this option is selected, you must provide the location of the key file as described in the Topic "The Process of Exporting and Sealing Management Packs" earlier in this module. You can optionally provide a company name and copyright that should be added to the sealed Management Pack. You then specify the output path to where the Management Pack will be saved. |
| Management Group                    | Configure Visual Studio to connect to the Management Group where the Management Pack will be deployed. This is useful because you can then configure Visual Studio to automatically deploy the Management Pack during the build process. When configuring the Management Group, you specify a Management Server name and relevant credentials that should be used to connect to the Management Group. This information is then stored in Visual Studio.                                                                                                                                                      |
| Deployment                          | A number of settings relating to how the project is deployed are available on this tab. For example, you can enable deployment versioning, which automatically increases the version number of the project each time it is deployed. You can also configure start actions by using options such as Deploy And Start The Operations Console or Deploy Projects To Default Management Group Only.                                                                                                                                                                                                              |

After you make any relevant changes to the Management Pack properties, you must right-click the tab and then click Save Selected Items to save any changes you made.

To build the Management Pack, you click the Build Solution option on the Build menu. This compiles the relevant Management Pack files and then creates the Management Pack in the location defined in the properties as described in the preceding table. During the build process, any errors or warnings that are generated are shown in the Error List pane. You can view detailed information relating to the error and warning, which in many cases includes information about how to fix the problem detected. You can also double-click an error or warning to open the associated Management Pack item. When the item is opened, the cursor appears at the beginning of the section where the problem was detected. This is very useful when troubleshooting build errors, because you do not need to find and open the associated Management Pack item.

## The Process of Authoring a Management Pack in VSAE and Adding a References and a Class

For the rest of this module, you will be guided though a number of steps in Visual Studio 2013 by using VSAE to create a Management Pack that measures network speed by transferring a file over the network.

To author a new Management Pack by using VSAE, you must first create a new project and then, from the Management Packs templates section, select the most appropriate Management Pack template. If, for example you need the Management Pack to be compatible with both Operations Manager 2007 R2 and Operations

Manager 2012 R2, you would select the Operations Manager 2007 R2 Management Pack template. If you will be using only the Management Pack with Operations Manager 2012 R2, you should select the Operations Manger 2012 R2 Management Pack Template.

### To author a Management Pack in VSAE and add references and a class, you must:

- Create a new project
- Select the Management Pack template
- Add Management Pack references in Solution Explorer
- Add a class by using the Add\New Item option

### Create the Management Pack in Visual Studio

Perform the following steps in Visual Studio to create a new Management Pack:

1. Open Visual Studio.
2. Click **File**, click **New**, and then click Project.
3. In the **New Project** dialog box that opens, click Management Pack.
4. From the details pane, click **Operations Manager 2012 R2 Management Pack**.
5. In the **Name** box, replace the existing text by typing **Network Speed**, and then click **OK**.

### Add References to the Management Pack

For the Management Pack to reference required elements from other Management Packs, you must add the references in the project. Perform the following steps in Visual Studio to add references to the Management Pack:

1. From the **Solution Explorer** pane, right-click References, and then click **Add Reference**.
2. In the **Add Reference** dialog box that opens, click the **Browse** tab.
3. On the Operations Manager media, browse to the **Management Packs** folder, click **Microsoft.SystemCenter.DataWarehouse.Library.mp**, and then click **OK**.
4. Right-click **References**, and then click **Add Reference** again.
5. In the **Add Reference** dialog box that opens, click the **Browse** tab.
6. On the Operations Manager media, browse to the **Management Packs** folder, click **System.Performance.Library.mp**, and then click **OK**.

### Add a Class to the Management Pack

For rules and monitors to be targeted appropriately in the Management Pack, you must also create a class. Perform the following steps in Visual Studio to add a class to the Management Pack:

1. From the **Solution Explorer** pane, right click the Network Speed solution name, click **Add**, and then click **New Item**.
2. In the **Add New Item – Network Speed** dialog box that opens, click **Class**.
3. In the **Name** box, replace the existing text with **TargetClass**, and then click **Add**.

- In the **TargetClass.mpx** window that opens, edit the **Class Type ID** section as shown in the following code.

```
<ClassType ID="Network_Speed.TargetClass" Base="Windows!
Microsoft.Windows.LocalApplication" Accessibility="Internal" Abstract="false"
Hosted="true" Singleton="false">
```

- Edit the **LanguagePacks** section as follows.

```
<DisplayString ElementID="Network_Speed.TargetClass">
<Name>Network Speed Target Class</Name>
<Description>Class to act as a target for sample rules and monitors.</Description>
</DisplayString>
```

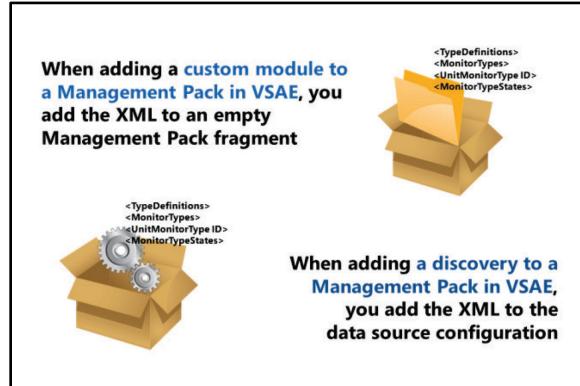
- Right click the **TargetClass.mpx** tab, and then click **Save TargetClass.mpx**.

## The Process of Adding a Custom Module and Discovery to the Management Pack

In the example in this topic, a custom probe action module is used in a Management Pack to run a Windows PowerShell script that will transfer a file over the network. The time taken to transfer the file is then used to measure network speed. The custom probe action module is used by a discovery, rule, and monitor in this Management Pack by using a custom data source. To facilitate this, custom module must be created in Visual Studio.

### Create a Custom Module

Perform the following steps in Visual Studio to create a custom module for the Management Pack:



- In the **Solution Explorer** pane, right-click the Network Speed solution name, click **Add**, then click **New Item**.
- In the **Add New Item – Network Speed** dialog box that opens, click **Empty Management Pack Fragment**.
- In the **Name** box, remove the existing text and type **Modules**, and then click **Add**.
- In the **Modules.mpx** window that opens, between the two **ManagementPackFragement** tags, add the following XML code.

```
<TypeDefinitions>
<ModuleTypes>
<DataSourceModuleType ID="Network_Speed.NetworkSpeedScheduled"
Accessibility="Public">
<Configuration>
<xsd:element minOccurs="1" name="Interval" type="xsd:integer" />
<xsd:element minOccurs="0" name="SyncTime" type="xsd:string" />
<xsd:element minOccurs="1" name="File" type="xsd:string" />
</Configuration>
<OverrideableParameters>
<OverrideableParameter ID="Interval" Selector="$Config/Interval$" ParameterType="int"
/>
<OverrideableParameter ID="SyncTime" Selector="$Config/SyncTime$"
ParameterType="string" />
```

```

<OverrideableParameter ID="File" Selector="$Config/File$" ParameterType="string" />
</OverrideableParameters>
<ModuleImplementation>
<Composite>
<MemberModules>
<DataSource ID="Scheduler"TypeID="System!System.Scheduler">
<Scheduler>
<SimpleRecurringSchedule>
<Interval>$Config/Interval$</Interval>
<SyncTime>$Config/SyncTime$</SyncTime>
</SimpleRecurringSchedule>
<ExcludeDates />
</Scheduler>
</DataSource>
<ProbeAction ID="Script"TypeID="Network_Speed.NetworkSpeed">
<File>$Config/File$</File>
</ProbeAction>
</MemberModules>
<Composition>
<Node ID="Script">
<Node ID ="Scheduler" />
</Node>
</Composition>
</Composite>
</ModuleImplementation>
<OutputType>Perf!System.Performance.Data</OutputType>
</DataSourceModuleType>
<ProbeActionModuleType ID="Network_Speed.NetworkSpeed" Accessibility="Internal"
Batching="false" PassThrough="false">
<Configuration>
<xsd:element minOccurs="1" name="File" type="xsd:string" />
</Configuration>
<ModuleImplementation Isolation="Any">
<Composite>
<MemberModules>
<ProbeAction ID="Script"TypeID="Windows!Microsoft.Windows.PowerShellProbe">
<ScriptName>NetworkSpeed.ps1</ScriptName>
<ScriptBody>
<![CDATA[
param($fileToRead)
$startTime = [DateTime]::Now
$streamReader = new-object System.IO.StreamReader($fileToRead)
$value = $streamReader.ReadToEnd()
$endTime = [DateTime]::Now
$timeInSeconds = $endTime.Subtract($startTime).TotalSeconds
$api = new-object -comObject "MOM.ScriptAPI"
$api.LogScriptEvent('NetworkSpeed.ps1',200,4,$timeInSeconds)
$bag = $api.CreatePropertyBag()
$bag.AddValue("TimeInSeconds",$timeInSeconds)
$bag
]]>
</ScriptBody>
<Parameters>
<Parameter>
<Name>FileToRead</Name>
<Value>$Config/File$</Value>
</Parameter>
</Parameters>
<TimeoutSeconds>300</TimeoutSeconds>
</ProbeAction>
<ConditionDetection ID="MapToPerf"
TypeID="Perf!System.Performance.DataGenericMapper">
<ObjectName>Network</ObjectName>
<CounterName>FileCopyTime</CounterName>
<InstanceName>$Config/File$</InstanceName>
<Value>$Data/Property[@Name='TimeInSeconds']$</Value>
</ConditionDetection>

```

```

</MemberModules>
<Composition>
<Node ID="MapToPerf">
<Node ID="Script" />
</Node>
</Composition>
</Composite>
</ModuleImplementation>
<OutputType>Perf!System.Performance.Data</OutputType>
<InputType>System!System.BaseData</InputType>
</ProbeActionModuleType>
</ModuleTypes>
</TypeDefinitions>

```

5. Right-click the **Modules.mpx** tab, and then click **Save Modules.mpx**.

### Create a Discovery

To discover the class, a discovery must be created in the Management Pack. Perform the following steps in Visual Studio to create a discovery:

1. From the **Solution Explorer** pane, right-click the Network Speed solution name, click Add, and then click **New Item**.
2. In the **Add New Item – Network Speed** dialog box that opens, click **Discovery**.
3. In the **Name** box, remove the existing text and type **Discovery**, and then click **Add**.
4. In the **Discovery.mptg** window that opens, click **NewDiscovery**.
5. From the **Properties** pane, in the **discovery Type** section, click **discovery Classes**, and then click the **ellipsis** button (...).
6. In the **Discovery Classes Collection Editor** window that opens, click **Add**.
7. In the properties section, click **Class**, and then click (...).
8. In the **Choose a Class** dialog box that opens, click **Network\_Speed.TargetClass**, and then click **OK**.
9. In the **Discovery Classes Collection Editor** window, click **OK**.
10. From the **Properties** pane, in the **General** section, remove the existing text in the **Display Name** box, and then type **Network Speed Discovery**.
11. In the **ID** box, remove the existing text, and then type **TargetDiscovery**.
12. Click **Target**, and then click (...).
13. In the **Choose a Class** dialog box that opens, click **Microsoft.Windows.Computer**, and then click **OK**.
14. From the **Properties** pane, in the **Modules** section, click **Data Source Type ID**, and then click (...).
15. In the **Choose a Data Source Module Type** dialog box that opens, click **Microsoft.Windows.FilteredRegistryDiscoveryProvider**, and then click **OK**.
16. From the **Properties** pane, in the **Modules** section, click **Data Source Configuration**, and then click (...).
17. In the **Enter Data Source Module Type** configuration dialog box that opens, enter the following XML between the two **Configuration** tags, and then click **OK**.

```

<ComputerName>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/NetworkName
$</ComputerName>
<RegistryAttributeDefinitions>
<RegistryAttributeDefinition>
<AttributeName>AppExists</AttributeName>

```

```

<Path>SOFTWARE\MPAuthor\CustomDataSource</Path>
<PathType>0</PathType>
<AttributeType>0</AttributeType>
</RegistryAttributeDefinition>
</RegistryAttributeDefinitions>
<Frequency>120</Frequency>
<ClassId>$MPElement[Name="Network_Speed.TargetClass"]$</ClassId>
<InstanceSettings>
<Settings>
<Setting>
<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
<Value>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Value>
</Setting>
<Setting>
<Name>$MPElement[Name="System!System.Entity"]/DisplayName$</Name>
<Value>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Value>
</Setting>
</Settings>
</InstanceSettings>
<Expression>
<SimpleExpression>
<ValueExpression>
<XPathQuery Type="String">Values/AppExists</XPathQuery>
</ValueExpression>
<Operator>Equal</Operator>
<ValueExpression>
<Value Type="String">True</Value>
</ValueExpression>
</SimpleExpression>
</Expression>

```

18. Right-click the **Discovery.mptg** tab, and then click **SaveDiscovery.mptg**.
19. Click the **File** menu, and then click **Save All**.

## The Process of Adding Monitors to a Management Pack in VSAE

To monitor the network speed, a unit monitor should be created in the Management Pack. You must first define the monitor type that will be used in the Management Pack and then add the unit monitor, which includes the under threshold and over threshold values that you configure for the monitor.

### Add a Monitor Type to the Management Pack

To add a monitor to the Management Pack, perform the following steps in VSAE:

1. From the **Solution Explorer** pane, right-click the Network Speed solution name, click **Add**, and then click **New Item**.
2. In the **Add New Item – Network Speed** dialog box that opens, click **Empty Management Pack Fragment**.
3. Remove the existing text in the **Name** box, type **ModuleTypes**, and then click **Add**.

#### When adding a monitor to a Management Pack in VSAE you:

- Create the monitor type by using an empty Management Pack fragment
- Add the monitor
- Configure the monitor properties

4. In the **ModuleTypes.mpx** window that opens, add the following XMS between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
<MonitorTypes>
<UnitMonitorType ID="Network_Speed.MonitorType.NetworkSpeed" Accessibility="Public">
<MonitorTypeStates>
<MonitorTypeState ID="UnderThreshold" NoDetection="false" />
<MonitorTypeState ID="OverThreshold" NoDetection="false" />
</MonitorTypeStates>
<Configuration>
<xsd:element minOccurs="1" name="Interval" type="xsd:integer" />
<xsd:element minOccurs="1" name="File" type="xsd:string" />
<xsd:element minOccurs="1" name="Threshold" type="xsd:double" />
</Configuration>
<OverrideableParameters>
<OverrideableParameter ID="Interval" Selector="$Config/Interval$" ParameterType="int" />
<OverrideableParameter ID="File" Selector="$Config/File$" ParameterType="string" />
<OverrideableParameter ID="Threshold" Selector="$Config/Threshold$" ParameterType="double" />
</OverrideableParameters>
<MonitorImplementation>
<MemberModules>
<DataSource ID="DS"TypeID="Network_Speed.NetworkSpeedScheduled">
<Interval>$Config/Interval$</Interval>
<File>$Config/File$</File>
</DataSource>
<ProbeAction ID="Probe"TypeID="Network_Speed.NetworkSpeed">
<File>$Config/File$</File>
</ProbeAction>
<ProbeAction ID="PassThrough"TypeID="System!System.PassThroughProbe" />
<ConditionDetection ID="FilterOverThreshold"TypeID="System!System.ExpressionFilter">
<Expression>
<SimpleExpression>
<ValueExpression>
<XPathQuery Type="Double">Value</XPathQuery>
</ValueExpression>
<Operator>GreaterEqual</Operator>
<ValueExpression>
<Value Type="Double">$Config/Threshold$</Value>
</ValueExpression>
</SimpleExpression>
</Expression>
</ConditionDetection>
<ConditionDetection ID="FilterUnderThreshold"TypeID="System!System.ExpressionFilter">
<Expression>
<SimpleExpression>
<ValueExpression>
<XPathQuery Type="Double">Value</XPathQuery>
</ValueExpression>
<Operator>Less</Operator>
<ValueExpression>
<Value Type="Double">$Config/Threshold$</Value>
</ValueExpression>
</SimpleExpression>
</Expression>
</ConditionDetection>
</MemberModules>
<RegularDetections>
<RegularDetection MonitorTypeStateID="UnderThreshold">
<Node ID="FilterUnderThreshold">
<Node ID="DS" />
</Node>
</RegularDetection>
<RegularDetection MonitorTypeStateID="OverThreshold">

```

```

<Node ID="FilterOverThreshold">
<Node ID="DS" />
</Node>
</RegularDetection>
</RegularDetections>
<OnDemandDetections>
<OnDemandDetection MonitorTypeStateID="UnderThreshold">
<Node ID="FilterUnderThreshold">
<Node ID="Probe">
<Node ID="PassThrough" />
</Node>
</Node>
</OnDemandDetection>
<OnDemandDetection MonitorTypeStateID="OverThreshold">
<Node ID="FilterOverThreshold">
<Node ID="Probe">
<Node ID="PassThrough" />
</Node>
</Node>
</OnDemandDetection>
</OnDemandDetections>
</MonitorImplementation>
</UnitMonitorType>
</MonitorTypes>
</TypeDefinitions>

```

5. Right click the **ModuleTypes.mpx** tab, and then click **Save ModuleTypes.mpx**.

### Add the Unit Monitor to the Management Pack

After you add the monitor type to the Management Pack, you can add the unit monitor to it. Perform the following steps in Visual Studio to add a unit monitor:

1. From **Solution Explorer** pane, right-click the Network Speed solution name, click **Add**, and then click **New Item**.
2. In the **Add New Item – Network Speed** dialog box that opens, click **Monitor (Unit)**.
3. Remove the existing text from the **Name** box and type **UnitMonitor**, and then click **Add**.
4. In the **UnitMonitor.mptg** window that opens, click **NewUnitMonitor**, and from the **Properties** pane, in the **Alert Settings** section, configure the following values:
  - Alert Auto Resolve: **True**
  - Alert Name: **Network Speed Test**
  - Alert Description: **Network Speed Test**
  - Alert On State: **Error**
5. In the General section, configure the following values:
  - Accessibility: **Public**
  - Category: **PerformanceHealth**
  - Comment: **Network Speed Test**
  - Description: **Network Speed Test**
  - Display Name **Network Speed Test**:
  - Enabled: **True**
  - ID: **Monitor.Network.Speed**
  - Target: **Network\_Speed.TargetClass**

6. In the **Unit Monitor** section, next to **Monitor Type ID**, click (...).
7. In the **Choose a Unit Monitor Type** dialog box that opens, click **Network\_Speed.MonitorType.NetworkSpeed**, and then click **OK**.
8. Next to the **Monitor Configuration** box, click (...).
9. In the **Enter Unit Monitor Type** configuration dialog box that opens, add the following XML between the **Configuration** tags, and then click **OK**.

```
<Interval>120</Interval>
<File>\<computer_name>\<share_name>\<file_name></File>
<Threshold>1</Threshold>
```



**Note:** Replace `<computer_name>`, `<share_name>` and `<file_name>` with appropriate values.

10. Next to **Monitor Operational States**, click (...).
11. In the **Map monitor conditions to health states** dialog box that opens, in the **Health State** column, click the **Under Threshold Value** drop-down list, click **Healthy**, and then click **OK**.
12. Next to **Parent Monitor ID**, click (...).
13. In the **Choose a Monitor** dialog box that opens, click **System.Healt.PerformanceState**, and then click **OK**.
14. Right-click the **UnitMonitor.mptg** tab, and then click **Save UnitMonitor.mptg**.

## The Process of Adding Rules to a Management Pack in VSAE

To collect the performance data used by the Management Pack, you must create a performance collection rule. You must also configure the properties of the rule to allow the rule to write performance data it collects to the operational database for views and to the data warehouse for reports.

### Add a Rule to the Management Pack

To add a rule to the Management Pack, perform the following steps in Visual Studio:

1. From the **Solution Explorer** pane, right-click the Network Speed solution name, click **Add**, and then click **New Item**.
2. In the **Add New Item – Network Speed** dialog box that opens, click **Rule (Performance Collection)**.
3. In the **Name** box, remove the existing text, type **CollectionRule**, and then click **Add**.
4. In the **CollectionRule.mptg** window that opens, click **NewPerformanceCollectionRule**.
5. From the **Properties** pane, in the **General** section, configure the following values:
  - o Comment: **Performance Collection Rule**

**When adding a rule to a Management Pack in VSAE, the following rule types are available:**

- Rule (Alert)
- Rule (Custom)
- Rule (Event Collection)
- Rule (Performance Collection)

**After adding the rule, you must then configure its properties, including:**

- ID
- Data Source Type ID

- Description: **Performance Collection Rule**
  - Display Name: **Collect Network Speed**
  - ID: **CollectNetworkSpeed**
  - Target: **Network\_Speed.TargetClass**
6. From the **Properties** pane, in the **Modules** section, next to the **Data Source Type ID** box, click (...).
  7. In the **Choose a Data Source Module Type** dialog box that opens, click **Network\_Speed.NetworkSpeedScheduled**, and then click **OK**.
  8. Next to **Data Source Configuration**, click (...), and in the **Enter Data Source Module Type Configuration** window that opens, enter the following XML between the **Configuration** tags and then click **OK**.

```
<Interval>120</Interval>
<SyncTime />
<File>\<computer_name>\<share_name>\<file_name></File>
```



**Note:** Replace `<computer_name>`, `<share_name>`, and `<file_name>` with appropriate values.

9. Right-click the **CollectionRule.mptg** tab, and then click **Save CollectionRule.mptg**.

## The Process of Adding Folders and Views to a Management Pack in VSAE

To view the results from the Network Speed monitor, you must add a folder and view to the Management Pack. The folder and view is then made available in the Operations console.

### Add a Folder and View to the Management Pack

To create a folder and view in the Management Pack, perform the following steps in Visual Studio:

1. From **Solution Explorer** pane, right-click the Network Speed solution name, click **Add**, and then click **New Item**.
2. In the **Add New Item – Network Speed** dialog box that opens, click **Folder & Folder Item**.
3. In the **Name** box, remove the existing text, type **ViewFolder**, and then click **Add**.
4. In the **ViewFolder.mpx** window that opens, remove the comment tags around the **FolderItem ID** line. The comment tags are `<!--and -->`.
5. In the **DisplayString** section, remove “**Network\_Speed.ViewFolder**”, and then type “**Network Speed**”.
6. Right-click the **ViewFolder.mpx tab**, and then click **Save Viewfolder.mpx**.
7. From **Solution Explorer** pane, right-click the Network Speed solution name, click **Add**, and then click **New Item**.
8. In the **Add New Item – Network Speed** dialog box that opens, click **View (Custom)**.

### To add folders and views to a Management Pack in VSAE:

- Add the **Folder & Folder Item** to the Management Pack
- Add the **View (Custom)** item to the Management Pack
- Configure the view type and target class

9. In the **Name** box, remove the existing text, type **TargetView**, and then click **Add**.
10. In the **TargetView.mptg** window that opens, click **NewView**.
11. In the **Properties** pane, in the **General** section, click the **Category** drop-down list, and then click **StateCollection**.
12. In the **Comment**, **Description**, and **Display Name** boxes, type **Network Speed State View**.
13. In the **ID** box, type **TargetView**.
14. Next to the **Target** box, click (...).
15. In the **Choose a Class** dialog box that opens, click **Network\_Speed.TargetClass**, and then click **OK**.
16. In the **View** section, next to the **View Type ID**, click (...).
17. In the **Choose a View Type** window dialog box that opens, click **Microsoft.SystemCenter.StateViewType**, and then click **OK**.
18. Next to the **View Folder** box, click (...).
19. In the **Choose a Folder** dialog box that opens, click **Network\_Speed.ViewFolder**, and then click **OK**.
20. Right-click the **TargetView.mptg** folder, and then click **Save TargetView.mptg**.

After configuring the various Management Pack items, you can build the Management Pack and import it into a Management Group. After you import the Management Pack, the Network Speed folder is visible in the Monitoring pane and includes a state view showing the health of the Network Speed monitor. In the Authoring pane, a Network Speed Test monitor will be added, which rolls up to the Performance monitor. You can edit the configuration of the monitor and modify the Interval, File, and Threshold values as required.

**Question:** You need to use VSAE to create a Management Pack that is compatible with Operations Manager 2007 R2 and Operations Manager 2012 R2. Which Management Pack template should you choose?

# Lab: Authoring Management Packs

## Scenario

Contoso, Ltd., has a number of in-house line-of-business applications for which there are no Management Packs available. You have been asked by your IT manager to create a Management Pack that includes all the necessary rules and monitors to enable effective monitoring of these applications. For some applications, you can create a Management Pack in the Operations console and then create the relevant rules and monitors for them. For more complex applications that also require a discovery mechanism, you can author a custom Management Pack by using the Visual Studio Authoring Extensions (VSAE).

## Objectives

After completing this lab, you will be able to:

- Create a Management Pack in the Operations console.
- Author a custom Management Pack by using VSAE.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machines:** 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-AP1, 10964C-LON-AP2

**User Name:** Contoso\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps.

1. On LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, in Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:
  - 10964C-LON-SQ1 (On LON-HOST1)
  - 10964C-LON-MS1 (On LON-HOST2)
  - 10964C-LON-AP1 (On LON-HOST1)
  - 10964C-LON-AP2 (On LON-HOST2)

 **Note:** In exercise 2 you use Visual Studio Authoring Extensions to author a new Management Pack for DinnerNow. It should be noted that this exercise is extensive and includes a number of code snippets that are used throughout the exercise to eliminate the possibility of error when manually editing the code. For this reason this exercise would be more suitable for developers who are already familiar with Visual Studio. If you would like to skip this exercise but

still review the results in Visual Studio and Operations Manager you can perform exercise 3 instead.

 **Note:** Before you start this lab, make sure that all Windows Services that are set to start automatically are running, except for the Microsoft .NET Framework NGEN v4.0.30319\_X86 and the .NET Framework NGEN v4.0.30319\_X64 services, because these services stop automatically when they are not being used.

## Exercise 1: Creating a Management Pack in the Operations console

### Scenario

For applications that do not require a discovery mechanism you decide to create the Management Pack using the Operations Console. You can then add the relevant rules and monitors that will be used to monitor the application and include overrides to adjust monitoring thresholds where necessary.

The main tasks for this exercise are as follows:

1. Create a Management Pack in the Operations console
2. Create a group to target overrides
3. Create monitors for the application
4. Create rules for the application
5. Create overrides to adjust monitoring thresholds
6. Create monitoring views
7. Test monitoring views

#### ► Task 1: Create a Management Pack in the Operations console

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration</b>
View	<b>Management Packs</b>

2. Using the **Create Management Pack** task, create a new Management Pack named **DinnerNow Custom Monitoring**.
3. Confirm the **DinnerNow Custom Monitoring** Management Pack was created.
4. Confirm the **DinnerNow Custom Monitoring** folder was created in the **Monitoring** pane.

#### ► Task 2: Create a group to target overrides

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>

Location	Value
Pane	<b>Authoring</b>
View	<b>Groups</b>

2. Use the **Create a New Group** task to create a new group with the following settings (all other settings should remain the default settings):
  - Name: **DinnerNow Production Servers**
  - Management Pack: **DinnerNow Custom Monitoring**
  - Explicit Members: Choose **Windows Computer** and then add **LON-AP2.CONTOSO.COM**
3. View the members of the **DinnerNow Production Servers** group, and confirm **LON-AP2.CONTOSO.COM** is included.

► **Task 3: Create monitors for the application**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Authoring\Management Pack Objects</b>
View	<b>Monitors</b>

2. Using the **Create a Monitor** task to create a new Unit Monitor with the following settings (all other settings should remain the default settings):
  - Monitor Type: Expand **Windows Performance Counters**, expand **Static Thresholds**, expand **Single Threshold**, and then click **Simple Threshold**
  - Management Pack: **DinnerNow Custom Monitoring**
  - Name: **DinnerNow Database Server CPU Utilization**
  - Monitor target: **Windows Server 2008 Operating System**
  - Parent Monitor: **Performance**
  - Monitor is enabled: **Cleared**
  - Performance Counter: **% Processor Time** from **Processor Information**
  - Interval: **5**
  - Threshold Value: **10.00**
  - Generate alerts for this monitor: **Selected**
  - Automatically resolve the alert when the monitor returns to a healthy state: **Cleared**

► **Task 4: Create rules for the application**

1. To perform this step, use the computer and the tool information shown in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Authoring\Management Pack Objects</b>
View	<b>Rules</b>

2. Using the **Create a Rule** task to create a new rule with the following settings (all other settings should remain the default settings):
  - Rule Type: From the **Alert Generating Rules** section, expand **Event Base**, and then select **NT Event Log (Alert)**
  - Management Pack: **DinnerNow Custom Monitoring**
  - Rule Name: **DinnerNow Database Unavailable**
  - Rule Target: **Windows Server 2008 Operating System**
  - Rule is enabled: **False**
  - Event ID: **5084**
  - Event Source: **MSSQL\$SQLEXPRESS**
  - Alert Suppression: **Event ID**

► **Task 5: Create overrides to adjust monitoring thresholds**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Authoring\Management Pack Objects</b>
View	<b>Monitors\Rules</b>

2. From the **Monitors** view, remove any scope, and then find the **DinnerNow Database Server CPU Utilization** monitor.
3. Override the monitor for the **DinnerNow Production Servers** group.
4. **Enable** the monitor.
5. Change the **Threshold** from **10** to **5**.
6. From the **Rules** view, remove any scope, and then find the **DinnerNow Database Unavailable** rule.
7. Override the monitor for the **DinnerNow Production Servers** group.
8. **Enable** the monitor.

► **Task 6: Create monitoring views**

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Monitoring</b>
Folder	<b>DinnerNow Custom Monitoring</b>

- Create an **Alert View** in the **DinnerNow Custom Monitoring** folder with the following settings:

- Name: **DinnerNow Database Unavailable Alerts**
- Show data contained in a specific group: **DinnerNow Production Servers**
- Select conditions: **with a specific name**
- Alert Name: **DinnerNow Database Unavailable**

- Create an **Alert View** in the **DinnerNow Custom Monitoring** folder with the following settings:

- Name: **DinnerNow Database Server CPU Utilization High Alerts**
- Show data contained in a specific group: **DinnerNow Production Servers**
- Select conditions: **with a specific name**
- Alert Name: **DinnerNow Database Server CPU Utilization**

► **Task 7: Test monitoring views**

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Monitoring</b>
Folder	<b>DinnerNow Custom Monitoring</b>

- On LON-AP2, use the DinnerNow SQL DBDetacher to detach the DinnerNow database.
- In the Operations console, open the **DinnerNow Database Unavailable Alerts** view from the **DinnerNow Custom Monitoring** folder.
- Open the **DinnerNow Database Unavailable** alert.
- Notice the **Repeat Count** value.
- Close the **DinnerNow Database Unavailable** alert.
- On LON-AP2, attach and then detach the **DinnerNow** database again.
- On LON-MS1, open the **DinnerNow Database Unavailable** alert.
- Notice the **Repeat Count** value has increased by one.



**Note:** It may take up to 5 minutes for the repeat count to increase.

10. Close the **DinnerNow Database Unavailable** alert.
11. On LON-AP2, attach the **DinnerNow** database.
12. In the Operations console open the **DinnerNow Database Server CPU Utilization High Alerts** view from the **DinnerNow Custom Monitoring** folder
13. Open the Health Explorer for the alert.
14. Select the monitor, and then review the state change events and details for the monitor.
15. Close the Health Explorer.

**Results:** After this exercise, you should have created a new Management Pack for DinnerNow by using the Operations console. You should have then created a group to target specific computers that host the DinnerNow components. Next, you should have created a rule and monitor for DinnerNow, and created an override to adjust the monitoring thresholds for the DinnerNow application.

## Exercise 2: Authoring a Management Pack by Using Visual Studio Authoring Extensions

### Scenario

For more complex applications that require discovery and new classes, you must use the Visual Studio Authoring Extensions to author a custom Management Pack.

The main tasks for this exercise are as follows:

1. Create the new Management Pack
2. Define the service model
3. Define relationships between the application and application components
4. Create the health model
5. Create the relationship mapper module
6. Define the health mode for the database discovery
7. Define the health model for the website discovery
8. Define the health model for the distributed application discovery
9. Define the health model dependency monitors
10. Define the URL probe composite data source
11. Define the custom URL probe monitor
12. Define the health model for the monitor
13. Define the health model for the rule
14. Define the views in the Operations console
15. Build and import the Management Pack

#### ► Task 1: Create the new Management Pack

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Menu	<b>File</b>
Option	<b>New Project</b>

2. Open a Visual Studio command prompt and browse to **C:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\CommonExtensions\Microsoft\Editor**
3. Type the following command and then press enter on the keyboard:

```
gacutil /i Microsoft.VisualStudio.Text.Logic.dll
```

4. Create the following folder structure on the C drive:

```
C:\Temp\DiinnerNow\2012TMP
```

5. Create a new project with the following properties by using **the Operations Manager 2007 R2 Management Pack template**:
  - Name: **CONTOSO.DinnerNow**
  - Location: **C:\Temp\DinnerNow\2012TMP**
  - Solution Name: **CONTOSO.DinnerNow**.
6. Edit the properties of the **CONTOSO.DinnerNow** solution and, on the **Management Group** tab, add a new connection by using **LON-MS1**.
7. Save the changes to the properties by using the **Save Selected Items** option.
8. Under the **CONTOSO.DinnerNow** solution, create the following folders:
  - **Classes**
  - **Discoveries**
  - **Modules and Types**
  - **Monitors**
  - **Rules**
  - **Views**
9. Add the following references to the solution:
  - **From \\LON-DC1\Media\Additional Management Packs\ add:**
  - **SQL Server\Microsoft.SQLServer.Library.mp**
  - **Internet Information Services 7\Microsoft.Windows.InternetInformationServices.2008.mp**
  - **Internet Information Services 7\Microsoft.Windows.InternetInformationServices.CommonLibrary.mp**
10. From C:\Program Files (x86)\System Center 2012 Visual Studio Authoring Extensions\References\OM2007R2,.add:
  - Microsoft.SystemCenter.DataWarehouseLibrary.mp
  - System.**Performance.Library.mp**
11. In the properties for the **Microsoft.SQLServer.Library**, change the **Alias** to **SQL**.
12. In the properties for the **Microsoft.Windows.InternetInformationServices.2008**, change the **Alias** to **IIS2008**.
13. In the properties for the **Microsoft.Windows.InternetInformationServices.CommonLibrary**, change the **Alias** to **IIS**.

#### ► Task 2: Define the service model

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Classes</b>

Location	Value
Action	Create a new Class

2. Create a new **Class** in the **Classes** folder that has the following setting:
  - a. Name: **Application.Class.mpx**
3. In the line that starts with **ClassType ID= "CONTOSO.DinnerNow.Application"**, change the **Base** element to "**Windows!Microsoft.Windows.LocalApplication**".
4. Change the **Hosted** element to "**true**".
5. In between the line that displays -- >, and the line that displays **<ClassType>** add the following four lines of XML code.

```

<Property ID="InstallPath" Key="false" Type="string" CaseSensitive="false"
MinLength="0" MaxLength="256"></Property>
<Property ID="DatabasePath" Key="false" Type="string" CaseSensitive="false"
MinLength="0" MaxLength="256"></Property>
<Property ID="Website" Key="false" Type="string" CaseSensitive="false" MinLength="0"
MaxLength="256"></Property>
<Property ID="DatabaseName" Key="false" Type="string" CaseSensitive="false"
MinLength="0" MaxLength="256"></Property>

```

6. In between the line that displays -- >, and the line that displays **</DisplayStrings>** add the following four lines of XML code.

```

<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="InstallPath">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="DatabasePath">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="Website">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="DatabaseName">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>

```

7. In the four **<Name>Install Path</Name>** sections replace **Install Path** with the following starting from the first:
  - a. Install Path
  - b. Database Path
  - c. Web Site
  - d. Database Name
  - e. Save the **Application.Class.mpx** file.
8. Add a new **Class** in the **Classes** folder that has the following setting:
  - Name: **DistributedApplication.Class.mpx**
  - In the line that begins with **ClassType ID="CONTOSO.DinnerNow.DistributedApplication"**, change the **Base** element to "**System!System.Service**".

- Change the **Singleton** element to “**true**”.
  - In the line that begins with **<DisplayString ElementID="CONTOSO.DinnerNow.DistributedApplication">**, change **CONTOSO.DinnerNow.DistributedApplication** to **DinnerNow**.
9. Save the **DistributedApplication.Class.mpx** file.

### ► Task 3: Define relationships between the application and application components

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Classes</b>
Action	<b>Create a new Class</b>

2. Create a new relationship in the **Classes** folder by using the following setting:
- Name: **DaContainsApp.Relationship.mpx**
  - Change the line that reads **<Source ID="Source" Type="">** to **<Source ID="Source" Type="CONTOSO.DinnerNow.DistributedApplication">**.
  - Change the line that reads **<Target ID="Target" Type="">** to **<Target ID="Target" Type="CONTOSO.DinnerNow.Application">**.
  - In the line that begins **<Name>DaContainsApp Relationship</Name>**, change the **DaContainsApp** relationship to **DinnerNow Distributed Application Contains Application**.
3. Save **DaContainsApp.Relationship.mpx**.
4. Create a new relationship in the **Classes** folder by using the following setting:
- Name: **AppContainsWebSite.Relationship.mpx**
  - Change the line **<Source ID="Source" Type="">** to **<Source ID="Source" Type="CONTOSO.DinnerNow.Application">**.
  - Change the line **<Target ID="Target" Type="">** to **<Target ID="Target" Type="IIS2008!Microsoft.Windows.InternetInformationServices.2008.WebSite">**.
  - In the line that reads **<Name>AppContainsWebSite Relationship</Name>**, change **AppContainsWebSite Relationship** to **DinnerNow Application Contains Web Site**.
5. Save **AppContainsWebSiteRelationship.mpx**.
6. Create a new relationship in the **Classes** folder by using the following settings:
- Name: **AppContainsDB.Relationship.mpx**
  - Change the line **<Source ID="Source" Type="">** to **<Source ID="Source" Type="CONTOSO.DinnerNow.Application">**.
  - Change the line **<Target ID="Target" Type="">** to **<Target ID="Target" Type="SQL!Microsoft.SQLServer.Database">**.

- In the line that reads **<Name>AppContainsDBRelationship Relationship</Name>**, change **AppContainsDBRelationship Relationship** to **DinnerNow Application Contains Database**.
- Save **AppContainsDBRelationship.mpx**.
  - Use the **Build Solution** option from the **BUILD** menu to test the build of the Management Pack.

#### ► Task 4: Create the health model

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Discoveries</b>
Action	<b>Create a new Discovery</b>

- Create a new **Discovery** in the **Discoveries** folder by using the following setting:
  - Name: **Discoveries.mptg**
- For the properties of the **NewDiscovery** item, configure the following:
  - Description: **Seed discovery for DinnerNow Application**
  - Display Name: **DinnerNow Application Discovery (Filtered Registry)**
  - ID: **CONTOSO.DinnerNow.Application.Discovery.FilteredRegistry**
  - Target: **Windows!Microsoft.Windows.Server.Computer**
  - Discovery Class: Add the **CONTOSO.DinnerNow.Application** class
  - Data Source ID: **Microsoft.Windows.FilteredRegistryDiscoveryProvider**
  - In the **Data Source Configuration**, add the following XML code.

```

<ComputerName>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/NetworkName
$</ComputerName>
 <RegistryAttributeDefinitions>
 <RegistryAttributeDefinition>
 <AttributeName>Installed</AttributeName>
 <Path>SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\DinnerNow</Path>
 <PathType>1</PathType>
 <AttributeType>0</AttributeType>
 </RegistryAttributeDefinition>
 <RegistryAttributeDefinition>
 <AttributeName>InstallPath</AttributeName>
 <Path>SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\DinnerNow</Path>
 <PathType>1</PathType>
 <AttributeType>1</AttributeType>
 </RegistryAttributeDefinition>
 <RegistryAttributeDefinition>
 <AttributeName>DatabasePath</AttributeName>
 <Path>SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo\%DinnerNow</Path>
 <PathType>1</PathType>
 <AttributeType>1</AttributeType>
 </RegistryAttributeDefinition>
 </RegistryAttributeDefinitions>

```

```

<Frequency>60</Frequency>
<ClassId>$MPElement[Name="CONTOSO.DinnerNow.Application"]$</ClassId>
<InstanceSettings>
 <Settings>
 <Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
<Value>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName$<Value>
<Setting>
 </Setting>
 <Setting>

<Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/InstallPath$</Name>
 <Value>$Data/Values/InstallPath$</Value>
 <Setting>
 <Setting>

<Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/DatabasePath$</Name>
 <Value>$Data/Values/DatabasePath$</Value>
 <Setting>
 <Setting>

<Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/Website$</Name>
 <Value>W3SVC/1</Value>
 <Setting>
 <Setting>

<Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/DatabaseName$</Name>
 <Value>DinnerNow</Value>
 <Setting>
 <Setting>
 <Name>$MPElement[Name="System!System.Entity"]/DisplayName$</Name>
 <Value>$Target/Property[Type="System!System.Entity"]/DisplayName$</Value>
 <Setting>
 </Setting>
 <Settings>
 </Settings>
 </InstanceSettings>
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <XPathQuery Type="String">Values/Installed</XPathQuery>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">true</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>

```

4. Save the **Discoveries.mptg** file.

► **Task 5: Create the relationship mapper module**

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Modules and Types</b>
Action	<b>Create a new Empty Management Pack Fragment</b>

- Create a new **Empty Management Pack Fragment** in the **Modules and Types** folder by using the following setting:

- Name: **FilteredRelationshipMapper.DataSource.mpx**
- Add the following XML code between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
<ModuleTypes>
 <DataSourceModuleType ID="CONTOSO.DinnerNow.FilteredRelationshipMapper"
 Accessibility="Internal" Batching="false">
 <Configuration>
 <IncludeSchemaTypes>
 <SchemaType>System!System.Discovery.MapperSchema</SchemaType>
 </IncludeSchemaTypes>
 <xsd:element minOccurs="1" name="Interval" type="xsd:integer" />
 <xsd:element minOccurs="0" name="SyncTime" type="xsd:string" />
 <xsd:element minOccurs="1" name="PropertyName" type="xsd:string" />
 <xsd:element minOccurs="1" name="PropertyValue" type="xsd:string" />
 <xsd:element minOccurs="1" name="RelationshipId" type="xsd:string" />
 <xsd:element minOccurs="0" name="SourceTypeId" type="xsd:string" />
 <xsd:element minOccurs="0" name="TargetTypeId" type="xsd:string" />
 <xsd:element minOccurs="1" name="SourceRoleSettings" type="SettingsType" />
 <xsd:element minOccurs="1" name="TargetRoleSettings" type="SettingsType" />
 </Configuration>
 <ModuleImplementation Isolation="Any">
 <Composite>
 <MemberModules>
 <DataSource ID="Scheduler"TypeID="System!System.Discovery.Scheduler">
 <Scheduler>
 <SimpleRecurringSchedule>
 <Interval>$Config/Interval$</Interval>
 <SyncTime>$Config/SyncTime$</SyncTime>
 </SimpleRecurringSchedule>
 <ExcludeDates />
 </Scheduler>
 </DataSource>
 <ConditionDetection ID="Filter"
 TypeID="System!System.ExpressionFilter">
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <Value Type="String">$Config/PropertyName$</Value>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">$Config/PropertyValue$</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>
 </ConditionDetection>
 </MemberModules>
 </Composite>
 </ModuleImplementation>
 </DataSourceModuleType>
</ModuleTypes>
</TypeDefinitions>

```

```

 </ConditionDetection>
 <ConditionDetection ID="Mapper"
TypeID="System!System.Discovery.RelationshipSnapshotDataMapper">
 <RelationshipId>$Config/RelationshipId$</RelationshipId>
 <SourceRoleSettings>$Config/SourceRoleSettings$</SourceRoleSettings>
 <TargetRoleSettings>$Config/TargetRoleSettings$</TargetRoleSettings>
 </ConditionDetection>
 </MemberModules>
 <Composition>
 <Node ID="Mapper">
 <Node ID="Filter">
 <Node ID="Scheduler" />
 </Node>
 </Node>
 </Composition>
 </Composite>
</ModuleImplementation>
<OutputType>System!System.Discovery.Data</OutputType>
</DataSourceModuleType>
</ModuleTypes>
</TypeDefinitions>

```

3. Save the **FilteredRelationshipMapper.DataSource.mpx** file.

#### ► Task 6: Define the health mode for the database discovery

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Discoveries</b>
Action	<b>Open the Discoveries.mptg file</b>

2. In Solution Explorer, from the **Discoveries** folder, open **Discoveries.mptg**, right-click in the white space area, and then add a new **Discovery (Custom)** template.
3. Configure the properties of the template as follows:
  - a. Display Name: **DinnerNow Database Discovery (Filtered Relationship Map)**
  - b. ID: **Database.Discovery.FilteredRelationshipMap**
  - c. Target: **CONTOSO.DinnerNow.Application**
  - d. Discovery Relationships: **CONTOSO.DinnerNow.AppContainsDB**
  - e. Data Source Type ID: **CONTOSO.DinnerNow.FileteredRelationshipMapper**
  - f. Data Source Configuration: Add the following XML code between the **Configuration** tags.

```

<Interval>60</Interval>
<PropertyName>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/DatabaseName$</PropertyName>

<PropertyValue>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/DatabaseName$</PropertyValue>
<RelationshipId>$MPElement[Name="CONTOSO.DinnerNow.AppContainsDB"]$</RelationshipId>
 <SourceRoleSettings>
 <Settings>

```

```

<Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
<Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
</Setting>
</Settings>
</SourceRoleSettings>
<TargetRoleSettings>
<Settings>
<Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
<Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
</Setting>
<Setting>

<Name>$MPElement[Name="SQL!Microsoft.SQLServer.ServerRole"]/InstanceName$</Name>
<Value>MSSQLSERVER</Value>
</Setting>
<Setting>

<Name>$MPElement[Name="SQL!Microsoft.SQLServer.Database"]/DatabaseName$</Name>
<Value>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/DatabaseName$</Value>
</Setting>
</Settings>
</TargetRoleSettings>

```

4. Save the **Discoveries.mptg** file.

#### ► Task 7: Define the health model for the website discovery

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Discoveries</b>
Action	<b>Open the Discoveries.mptg file</b>

2. In Solution Explorer, from the **Discoveries** folder, open the **Discoverie.mptg**, right-click in the white space area, and then add a new **Discovery (Custom)** template.
3. Configure the properties of the template as follows:
  - a. Display Name: **DinnerNow Web Site Discovery (Filtered Relationship Map)**
  - b. ID: **WebSite.Discovery.FilteredRelationshipMap**
  - c. Target: **CONTOSO.DinnerNow.Application**
  - d. Discovery Relationships: **CONTOSO.DinnerNow.AppContainsWebSite**
  - e. Data Source Type ID: **CONTOSO.DinnerNow.FileteredRelationshipMapper**
  - f. Data Source Configuration: Add the following XML code between the **Configuration** tags.

```

<Interval>60</Interval>
<PropertyName>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website$</Proper
tyName>
<PropertyValue>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website$</Prope
rtyValue>
<RelationshipId>$MPElement[Name="CONTOSO.DinnerNow.AppContainsWebSite"]$</Relationshi
pId>
 <SourceRoleSettings>
 <Settings>
 <Setting>

 <Name>$MPELEMENT[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
 <Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
 </Setting>
 </Settings>
 </SourceRoleSettings>
 <TargetRoleSettings>
 <Settings>
 <Setting>

 <Name>$MPELEMENT[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
 <Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
 </Setting>
 </Settings>
 </TargetRoleSettings>
 </Settings>
 </SourceRoleSettings>
 </Settings>
 </SourceRoleSettings>
<Name>$MPELEMENT[Name="IIS!Microsoft.Windows.InternetInformationServices.WebSite"]/Si
teID$</Name>
<Value>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website$</Value>
 </Setting>
 </Settings>
</TargetRoleSettings>

```

4. Save the **Discoveries.mptg** file.

#### ► Task 8: Define the health model for the distributed application discovery

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Discoveries</b>
Action	<b>Open the Discoveries.mptg file</b>

- In Solution Explorer, from the **Discoveries** folder, open **Discoverie.mptg**, right-click in the white space area, and add a new **Discovery (Custom)** template.
- Configure the properties of the template as follows:
  - Display Name: **DinnerNow Distributed Application Discovery (Group Populator)**
  - ID: **CONTOSO.DinnerNow.DistributedApplication.Discovery.GroupPopulator**
  - Target: **CONTOSO.DinnerNow.DistributedApplication**
  - Discovery Relationships: **CONTOSO.DinnerNow.DaContainsApp**
  - Data Source Type ID: **Microsoft.SystemCenter.GroupPopulator**

- f. Data Source Configuration: Add the following XML code between the **Configuration** tags.

```

RuleId>$MPElement$</RuleId>

<GroupInstanceId>$MPElement[Name="CONTOSO.DinnerNow.DistributedApplication"]$</GroupInstanceId>
 <MembershipRules>
 <MembershipRule>

 <MonitoringClass>$MPElement[Name="CONTOSO.DinnerNow.Application"]$</MonitoringClass>

 <RelationshipClass>$MPElement[Name="CONTOSO.DinnerNow.DaContainsApp"]$</RelationshipClass>
 </MembershipRule>
 </MembershipRules>

```

4. Save the **Discoveries.mptg** file.

#### ► Task 9: Define the health model dependency monitors

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Monitors</b>
Action	<b>Add a new Monitor (Dependency)</b>

- From the **Monitors** folder, add a new **Monitor (Dependency)** item with the following setting:

- Name: **Monitors.mptg**
- Configure the NewDependencyMonitor properties as follows:
    - Display Name: **DinnerNow Database Dependency Monitor**
    - ID: **Database.DependencyMonitor**
    - Target: **CONTOSO.DinnerNow.Application**
    - Health Roll-up Algorithm: **WorstOf**
    - Relationship Type: **CONTOSO.DinnerNow.AppContainsDB**
    - Member Monitor: **Health!System.Health.AvailabilityState**
    - Member Unavailable: **Roll up as error**
    - Parent Monitor ID: **Health!System.Health.EntityState**

- Save the **Monitors.mptg** file.
- Right-click in the white space area of the **Monitor.mptg** window, and then add a new **Monitor (Dependency)** template.
- Configure the NewDependencyMonitor properties as follows:
  - Display Name: **DinnerNow Web Site Dependency Monitor**
  - ID: **WebSite.DependencyMonitor**

- c. Target: **CONTOSO.DinnerNow.Application**
  - d. Health Roll-up Algorithm: **WorstOf**
  - e. Relationship Type: **CONTOSO.DinnerNow.AppContainsWebite**
  - f. Member Monitor: **Health!System.Health.AvailabilityState**
  - g. Member Unavailable: **Roll up as error**
  - h. Parent Monitor ID: **Health!System.Health.EntityState**
7. Save the **Monitors.mptg** file.
8. Right-click in the white space area of the **Monitor.mptg** window, and then add a new **Monitor (Dependency)** template.
9. Configure the **NewDependencyMonitor** properties as follows:
- a. Display Name: **DinnerNow Application Dependency Monitor**
  - b. ID: **Application.DependencyMonitor**
  - c. Target: **CONTOSO.DinnerNow.DistributedApplication**
  - d. Health Roll-up Algorithm: **WorstOf**
  - e. Relationship Type: **CONTOSO.DinnerNow.DaContainsApp**
  - f. Member Monitor: **Health!System.Health.AvailabilityState**
  - g. Member Unavailable: **Roll up as error**
  - h. Parent Monitor ID: **Health!System.Health.EntityState**
10. Save the **Monitors.mptg** file.

#### ► Task 10: Define the URL probe composite data source

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Modules and Types</b>
Action	<b>Add a new Management Pack Fragment</b>

2. From the **Modules and Types** folder, add a new Management Pack fragment item by using the following setting:
- a. Name: **UrlProbe.DataSource.mpx**
  - b. Add the following XML code between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
 <ModuleTypes>
 <DataSourceModuleType ID="CONTOSO.DinnerNow.URLProbe" Accessibility="Internal"
Batching="false">
 <Configuration>
 <xsd:element minOccurs="1" name="URL" type="xsd:string" />
 </Configuration>
 </DataSourceModuleType>
 </ModuleTypes>
</TypeDefinitions>

```

```

<ModuleImplementation Isolation="Any">
 <Composite>
 <MemberModules>
 <DataSource ID="Scheduler"TypeID="System!System.SimpleScheduler">
 <IntervalSeconds>60</IntervalSeconds>
 <SyncTime>00:00</SyncTime>
 </DataSource>
 <ProbeAction ID="PowerShell"
TypeID="Windows!Microsoft.Windows.PowerShellPropertyBagProbe">
 <ScriptName>CONTOSO.DinnerNow.URLProbe.ps1</ScriptName>
 <ScriptBody><! [CDATA[
param($URL)
$req = [System.Net.HttpWebRequest]::Create($URL);
$req.Credentials = [System.Net.CredentialCache]::DefaultCredentials
$res = $req.GetResponse();
$api = New-Object -comObject 'MOM.ScriptAPI'
$bag = $api.CreatePropertyBag()
if ($res.StatusCode -eq 200){
 $bag.AddValue('Match','True')
} else{
 $bag.AddValue('Match','False')
}
$bag
]]></ScriptBody>
 <Parameters>
 <Parameter>
 <Name>URL</Name>
 <Value>$Config/URL$</Value>
 </Parameter>
 </Parameters>
 <TimeoutSeconds>30</TimeoutSeconds>
 </ProbeAction>
 </MemberModules>
 <Composition>
 <Node ID="PowerShell">
 <Node ID="Scheduler" />
 </Node>
 </Composition>
 </Composite>
</ModuleImplementation>
<OutputType>System!System.PropertyBagData</OutputType>
</DataSourceModuleType>
</ModuleTypes>
<TypeDefinitions>

```

3. Save the **UrlProbe.DataSource.mpx** file.

► **Task 11: Define the custom URL probe monitor**

- To perform this step, use the computer and tool information that is shown in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Modules and Types</b>
Action	<b>Add a new Management Pack Fragment</b>

- From the **Modules and Types** folder, add a new Management Pack fragment item by using the following setting:

- Name: **URLProbe.MonitorType.mpx**
- Add the following XML code between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
 <MonitorTypes>
 <UnitMonitorType ID="CONTOSO.DinnerNow.URLProbe.MonitorType"
Accessibility="Internal">
 <MonitorTypeStates>
 <MonitorTypeState ID="DOWN" NoDetection="false" />
 <MonitorTypeState ID="UP" NoDetection="false" />
 </MonitorTypeStates>
 <Configuration>
 <xsd:element minOccurs="1" name="URL" type="xsd:string" />
 </Configuration>
 <MonitorImplementation>
 <MemberModules>
 <DataSource ID="URLPROBE"TypeID="CONTOSO.DinnerNow.URLProbe">
 <URL>$Config/URL$</URL>
 </DataSource>
 <ConditionDetection ID="CheckDOWN"
TypeID="System!System.ExpressionFilter">
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <XPathQuery Type="String">Property[@Name="Match"]</XPathQuery>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">False</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>
 </ConditionDetection>
 <ConditionDetection ID="CheckUP"TypeID="System!System.ExpressionFilter">
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <XPathQuery Type="String">Property[@Name="Match"]</XPathQuery>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">True</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>
 </ConditionDetection>
 </MemberModules>
 </MonitorImplementation>
 </UnitMonitorType>
 </MonitorTypes>
</TypeDefinitions>

```

```

</MemberModules>
<RegularDetections>
 <RegularDetection MonitorTypeStateID="DOWN">
 <Node ID="CheckDOWN">
 <Node ID="URLPROBE" />
 </Node>
 </RegularDetection>
 <RegularDetection MonitorTypeStateID="UP">
 <Node ID="CheckUP">
 <Node ID="URLPROBE" />
 </Node>
 </RegularDetection>
</RegularDetections>
<MonitorImplementation>
</UnitMonitorType>
</MonitorTypes>
</TypeDefinitions>

```

3. Save the URLProbe.MonitorType.mpx file.

► **Task 12: Define the health model for the monitor**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Monitors</b>
Action	<b>Add a new Monitor (Unit)</b>

2. In Solution Explorer, from the **Monitors** folder, right-click **Monitors.mptg**, and then click **Open**.
3. Add a new Monitor (Unit) template.
4. Configure the properties of **NewUnitMonitor** as follows:
  - a. Display Name: **DinnerNow Website URL Probe Monitor**
  - b. ID: **Website.UrlProbeMonitor**
  - c. Target: **CONTOSO.DinnerNow.Application**
  - d. Monitor Type ID: **CONTOSO.DinnerNow.URLProbe.MonitorType**
  - e. Parent Monitor ID: **Health!System.Health.AvailabilityState**
5. Configure the **Monitor Operational States** setting so that the health state for UP is set to **Healthy**.
6. Configure the monitor configuration with the following XML code between the **Configuration** tags.

```
<URL>http://localhost/DinnerNow/</URL>
```

7. Save the Monitors.mptg file.

► **Task 13: Define the health model for the rule**

1. To perform this step, use the computer and tool information in the following table.

Location	Value

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Rules</b>
Action	<b>Add a new Snippet Template</b>

1. In Solution Explorer, from the **Rules** folder, add a new Snippet Template item with the following setting:
  - a. Name: **WindowsPerformanceCounters.templatesnippet**
  - b. Replace the line that reads **<Name>Collection rule for performance counter #text('Perf Counter Name')#.</Name>** with **<Name>#text('Rule Id')# - Snippet Generated</Name>**.
  - c. Replace the text that reads **Target="#alias('Microsoft.Windows.Library')#!Microsoft.Windows.Computer"** with **Target="CONTOSO.DinnerNow.Application"**.
  - d. Replace the text that reads **<ComputerName>\$Target/Property[Type ...** with **<ComputerName>\$Target/Host/Property[Type ....**
2. Save the **WindowsPerformanceCounters.templatesnippet** file.
3. In Solution Explorer, add a Snippet Data item to the Rules folder with the following setting:
  - Name: **WindowsPerformanceCounterRules.mpsd**
4. Use the **Select Snippet Type** button to select the **Rules\WindowsPerformanceCounters** type.
5. Use the **Click here to add a new item** link to add a new item with the following settings:
  - RuleID: **WPC.Process.WorkingSet.w3wp**
  - Perf Counter Name: **Process**
  - Perf Object Name: **Working Set**
  - Perf Instance Name: **w3wp**
  - Collection Frequency: **900**
6. Use the **Click here to add a new item** link to add a new item the following settings:
  - RuleID: **WPC.WebService.CurrentConnections.DefaultWebSite**
  - Perf Counter Name: **Web Service**
  - Perf Object Name: **Current Connections**
  - Perf Instance Name: **Default Web Site**
  - Collection Frequency: **900**
7. Save the **WindowsPerformanceRules.mpsd** file.

► **Task 14: Define the views in the Operations console**

1. To perform this step, use the computer and tool information in the following table.

Location	Value

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Folder	<b>Views</b>
Action	<b>Add a new Folder &amp; Folder Item</b>

2. In Solution Explorer, from the **Views** folder, add a new **Folder & Folder Item** with the following settings
  - Name: **Folder.mpx**
  - In the line that reads **<Name>Folder Folder</Name>**, replace **Folder Folder** with **\_CONTOSO.DinnerNow**.
3. Save the **Folder.mpx** file.
4. In Solution Explorer, from the **Views** folder, add a new **View (Custom)** item with the following setting:
  - Name: **Views.mptg**
5. Configure the **NewView** properties as follows:
  - Display Name: **Application State**
  - ID: **ApplicationStateView**
  - Target: **CONTOSO.DinnerNow.Application**
  - View Folder: **Contoso.DinnerNow.Folder**
  - View Type ID: **SC!Microsoft.SystemCenter.StateViewType**
6. Save the **Views.mptg** file.
7. Right-click in the white space area of the **Views.mptg** window, and then add a new **View (Custom)** template.
8. Configure the **NewView** properties as follows:
  - Display Name: **DinnerNow Distributed Application Diagram**
  - ID: **DistributedApplicationDiagram**
  - Target: **CONTOSO.DinnerNow.DistributedApplication**
  - View Folder: **Contoso.DinnerNow.Folder**
  - View Type ID: **SC!Microsoft.SystemCenter.DiagramViewType**
9. Save the **Views.mptg** file.

► **Task 15: Build and import the Management Pack**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Manu	<b>File</b>
Action	<b>Save All</b>

2. From the **File** menu, use the **Save All** option to save the project.
3. From the **Build** menu, use the **Build Solution** option to build the **Management Pack**.
4. Exit Visual Studio.
5. Open the Operations console on LON-MS1.
6. Import the **CONTOSO.DinnerNow.xml** Management Pack from **\LON-AP1\c\$\Temp\Contoso.DinnerNow\2012TMP\Contoso.DinnerNow\Contoso.DinnerNow\bin\Debug**.
7. From the **Monitoring** pane, expand the **\_CONTOSO.DinnerNow** folder, and then open the **Application State** view.
8. Wait for the **DinnerNow** application to be discovered and displayed in a healthy state.
9. Open the **DinnerNow Distributed Application** view and expand the components groups to review the application components that have been discovered.

**Results:** After this exercise, you should have created a Management Pack by using VSAE. Included in the Management Pack should be various discoveries, rules, monitors, and views that are used to discover and monitor the DinnerNow application that is running on LON-AP2. After you import the Management Pack, you should be able to confirm that the DinnerNow application is discovered and is displayed in a healthy state.

## Exercise 3: Alternative to Exercise 2

### Scenario

This exercise is an alternative to exercise 2 and will allow you to review the results from creating and deploying the DinnerNow Management Pack.

The main tasks for this exercise are as follows:

1. Open the Visual Studio DinnerNow project
2. Build and import the Management Pack

#### ► Task 1: Open the Visual Studio DinnerNow project

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Administrator: VS2013 x64 Native Tools Command Prompt</b>

2. Open a Visual Studio command prompt and browse to **C:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\CommonExtensions\Microsoft\Editor**
3. Type the following command and then press enter on the keyboard:

```
gacutil /i Microsoft.VisualStudio.Text.Logic.dll
```

4. From the desktop open **Visual Studio 2013**.
5. Open the **Contoso.DinnerNow** solution from the **C:\Module 9\Contoso.DinnerNow** folder.

#### ► Task 2: Build and import the Management Pack

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-AP1</b>
Tool	<b>Visual Studio 2013</b>
Manu	<b>File</b>
Action	<b>Save All</b>

2. From the **File** menu, use the **Save All** option to save the project.
3. From the **Build** menu, use the **Build Solution** option to build the **Management Pack**.
4. Exit Visual Studio.
5. Open the Operations console on LON-MS1.
6. Import the **CONTOSO.DinnerNow.xml** Management Pack from **\LON-AP1\C\$\Module 9\Contoso.DinnerNow\Contoso.DinnerNow\bin\Debug**.
7. From the **Monitoring** pane, expand the **\_CONTOSO.DinnerNow** folder, and then open the **Application State** view.

8. Wait for the **LON-AP2.CONTOSO.COM** computer to be discovered and displayed in a healthy state.
9. Review the DinnerNow information in the **Detail View**.
10. Open the **DinnerNow Distributed Application Diagram** view and expand the components groups to review the application components that have been discovered.

**Results:** After this exercise you should have loaded the Visual Studio project into Visual Studio 2013 and then built the DinnerNow Management Pack. You should then have imported the Management Pack into Operations Manager and confirmed that the DinnerNow application is being monitored.

**Question:** What can Groups be used for in Operations Manager?

**Question:** You need to add a folder to a Management Pack in VSAE. What item should you select?

# Module Review and Takeaways

## Review Question(s)

**Question:** Name the three monitor types that can be added to a Management Pack in VSAE?

## Real-world Issues and Scenarios

### Authoring Management Packs by Using Visual Studio Authoring Extensions

For more information about authoring Management Packs by using Visual Studio Authoring Extensions, go to the following TechNet link: <http://go.microsoft.com/fwlink/?LinkId=391278>

## Tools

Although not as comprehensive as the Visual Studio Authoring Tools in authoring Management Packs you can also create Management Packs from a Visio. This allows you to visually design a Management Pack using shapes in Visio.



# Module 10

## Integrating Operations Manager with Other System Center Components

### Contents:

Module Overview	10-1
<b>Lesson 1: Service Manager Integration</b>	<b>10-2</b>
<b>Lesson 2: Data Protection Manager Integration</b>	<b>10-10</b>
<b>Lesson 3: Orchestrator Integration</b>	<b>10-16</b>
<b>Lab: Configuring System Center Integration</b>	<b>10-25</b>
Module Review and Takeaways	10-35

## Module Overview

Microsoft System Center 2012 R2 consists of several components that provide complete management of the IT environment. This includes the server and desktop infrastructure and the networking infrastructure that binds them. You can also manage client devices by using System Center 2012 R2.

You should integrate System Center 2012 R2 components to provide seamless management of the IT environment from both a cloud and datacenter perspective. This provides easier and more flexible management of the cloud and datacenter environment, and enables automation of many manual processes.

In this module, you will learn several key features of other System Center 2012 R2 components. This includes the benefits that are achieved when integrating Microsoft System Center 2012 Operations Manager with them.

### Objectives

After completing this module, students will be able to:

- Describe Microsoft System Center 2012 R2 Service Manager and configure integration with Operations Manager.
- Describe System Center 2012 R2 Data Protection Manager and configure integration with Operations Manager.
- Describe Microsoft System Center 2012 R2 Orchestrator and configure integration with Operations Manager.

## Lesson 1

# Service Manager Integration

Service Manager provides the ability to standardize datacenter processes and best practices such as those found in Microsoft Operations Framework and the IT Infrastructure Library (ITIL). By integrating Service Manager with other System Center 2012 R2 components, you can extend the capabilities of Service Manager further to provide management of processes running in the datacenter and cloud.

To understand the benefits of integrating Service Manager with Operations Manager, you should first understand Service Manager's key features and capabilities.

When configuring integration between Service Manager and Operations Manager, you must also understand how Service Manager Connectors are configured to synchronize Operations Manager data with Service Manager's CMDB.

Finally, to ensure that Service Manager remains in an optimal state, it is important that you monitor it effectively with Operations Manager via the appropriate Management Pack.

### Lesson Objectives

After completing this lesson, students will be able to:

- Describe Service Manager functionality and capabilities.
- Describe how Service Manager integrates with other System Center 2012 components.
- Describe the Operations Manager Connector functionality and capabilities.

Describe the Operations Manager Management Pack for Service Manager functionality and capabilities.

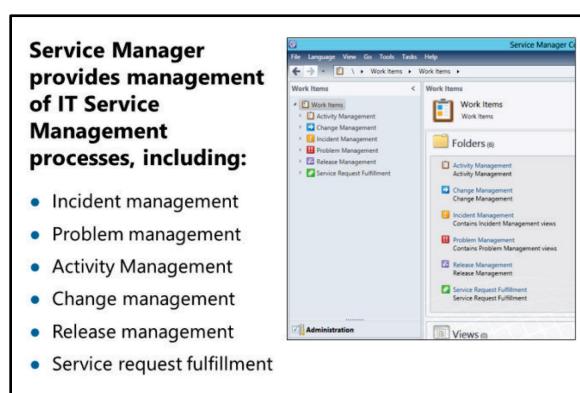
### Overview of Service Manager

Service Manager is an IT Service Management solution that lets you manage and automate business processes that organizations have adopted through best practices, such as ITIL and Microsoft Operations Framework. Service Manager provides management of the IT Service Management processes: described in the following sections.

#### Incident Management

In the IT environment, an *incident* is an unplanned disruption or degradation of service. For example, a user's access to the intranet website is blocked because the password was entered incorrectly too many times. When troubleshooting and resolving incidents, there is much information that must be collected and recorded. This includes user details such as the following:

- Name
- Department
- Contact number
- Incident details



- Computer name that users are experiencing problems with
- Application that users are trying to access
- Description of the incident (including steps to reproduce it)
- Error codes or messages that are generated when the incident occurs

Incident Management in Service Manager provides a method of recording this information and managing the complete life cycle of an incident. This includes the following:

- Managing incident escalations
- Creating, resolving, and closing incidents
- Managing activities that are performed when resolving incidents
- Providing a searchable troubleshooting knowledge
- Resolving reoccurring incidents

### **Problem Management**

A *problem* in the IT environment can be thought of as the cause of one or more incidents. In Service Manager, *Problem records* are created to manage the life cycle of a problem. For example, multiple incidents that relate to a problem can be grouped in a problem record. This helps manage incidents and problems, because when a problem record is resolved, that resolution can automatically resolve any related incidents. Similar to incidents, when a problem record is created, details of related items, such as computers, services, and people, can be included. By providing a method of viewing and managing the problem's effect in the environment, problem records help you manage the IT environment.

### **Change Management**

Managing changes in the IT environment is an important process. For example, before you apply a major configuration change to a business-critical application, the change must be evaluated by relevant staff and then approved. By recording and managing changes in the environment, you reduce downtime and problems that occur as a result of those changes. Service Manager handles changes by using *change requests*. A change request is created by using a configurable template, such as the Major Change Request template. When you create a change request, details of the change to implement are recorded. This includes the following:

- Scheduled start date and end date
- Activities performed as part of the change
- Related items that the change affects

### **Release Management**

*Release Management* in Service Manager provides a method for managing change requests and activities. Being able to manage change requests and activities is important, because an upgrade to an application might involve several changes and activities, such as the following:

- Testing the upgrade in development
- Preparing the production environment
- Upgrading clients
- Upgrading servers

By using release records in Service Manager, you can group and schedule approved change requests for deployment after they are tested and confirmed safe to release.

### **Service Level Management**

The ability to track and report on service levels in the IT environment is a very important function in understanding whether service level goals are met. For example, an organization's incident management policy or service-level agreement (SLA) might state that all incidents with an impact rating of High must be resolved within three hours. By using Service Level Management in Service Manager, you can track and report on service levels such as these and send notifications when service levels are breached.

### Service Request Fulfillment

A service request in Service Manager includes one or more request offerings and/or service offerings. *Request offerings* let you create preauthorized services for users, for example, the ability to raise an incident from the Service Manager Self-Service portal.

When you create a request offering, you configure prompts for users to complete that relate to the offering, such as incident title, category, and priority. Users then enter the relevant information when they use the request offering. This information is captured in Service Manager and used when the incident is created.

Multiple request offerings can be grouped into a *service offering*. This is useful when similar request offerings, such as Database Backup and Database Restore, are made available to users. Request offerings and service offerings are managed by using a Service Catalog in Service Manager. This lets you scope user access to the offerings based on the user's user role membership in Service Manager.

### Self-Service Portal

The *Service Manager Self-Service Portal* is a web interface that lets users submit and review service requests. When service offerings and request offerings are configured in Service Manager, they are published to the Self-Service Portal. By using the Self-Service Portal to manage service requests, much of the administration overhead is removed. This is because users can submit relevant service request information by completing forms in the Self-Service Portal instead of contacting the helpdesk. This also gives users more control when submitting service requests. It reduces errors or missing information by making certain fields mandatory in the service request form.

For more information about Service Manager, go to the following link:



### Service Manager

<http://go.microsoft.com/fwlink/?LinkId=321902>

## How Service Manager Integrates with other System Center 2012 R2 Components

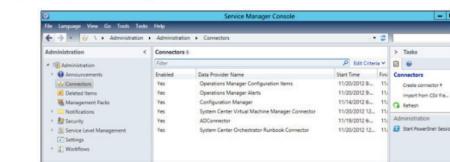
Service Manager integrates with other System Center 2012 R2 components by using connectors. A *connector* in Service Manager provides the details that are required to connect to the relevant component and synchronize data between Service Manager and the connected component.

In System Center 2012 R2, Service Manager provides connectors for the following System Center 2012 R2 components:

- Configuration Manager
- Operations Manager
- Orchestrator

### Service Manager integrates with other System Center components by using connectors:

- Configuration Manager connector
- Operations Manager connector
- Orchestrator connector
- Virtual Machine Manager connector
- Active Directory connector



- System Center 2012 Virtual Machine Manager

In addition, there is a connector for Service Manager that synchronizes data from Active Directory Domain Services (AD DS). This is required for Service Manager to manage the relationship between configuration items such as the following:

- Computers
- Software
- Users
- Work items, such as incidents, problems, and change requests

For more information about Service Manager Connectors, go to the following link:

#### **Service Manager Connectors**

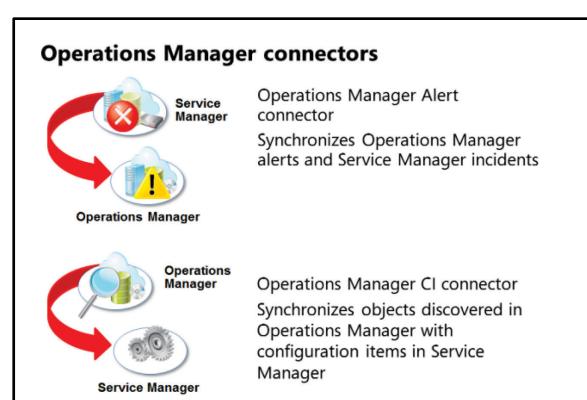
<http://go.microsoft.com/fwlink/?LinkId=321903>

## Service Manager Connectors for Operations Manager

Service Manager provides two connectors for Operations Manager: the Operations Manager Alert connector, and the Operations Manager Configuration Items (CI) connector.

### Operations Manager Alert Connector

Use the Operations Manager Alert connector to create incidents in Service Manager that are based on alerts that were generated in Operations Manager. Operations Manager can synchronize alerts and incidents so that when an incident is resolved in Service Manager, the alert is resolved automatically in Operations Manager. In the same manner, if an alert is closed in Operations Manager, the incident is resolved automatically in Service Manager. By automating incident creation in Service Manager, you reduce administrative overhead, because you can use Service Manager templates to automatically populate fields in the incident form with data from the Operations Manager alert.



### Operations Manager CI Connector

Use the Operations Manager CI connector to synchronize objects that are discovered in Operations Manager, with configuration items in Service Manager. Then you can use these configuration items with work items such as incidents or change requests. As Management Packs are imported into Operations Manager, the Operations Manager agent discovers objects such as hard drives and websites on computers that they manage. For Service Manager to reference these objects when associating them with configuration items, you must import the relevant Operations Manager Management Packs into Service Manager. Unless you import the relevant Management Pack, objects from Operations Manager are not synchronized with configuration items in Service Manager.

### Creating an Operations Manager Alert Connector

Use the Operations Manager Alert Connector wizard to create an Alert connector to Operations Manager. Open the wizard by clicking Create connector from the Tasks pane in Service Manager, which is in the

Connectors node in the Administration pane of the Service Manager Console. When you create the connector, you must supply several connection settings, which are described in the following table.

Operations Manager Alert Connector wizard page	Description
Server Details	<p>Specify the server name of the Operations Manager Management Server and the credentials that should be used to connect to the server. The credentials that are specified here are in the form of a Run As account. The account that you use to connect to the Operations Manager Management Server must have the following permissions:</p> <ul style="list-style-type: none"> <li>• Be a domain account.</li> <li>• Be a member of the user's local security group on the Service Manager Management Server.</li> <li>• Be a member of the Administrator user role in Operations Manager.</li> <li>• Be a member of the Advanced Operator user role in Service Manager.</li> </ul> <p>A Test connection button is available, which is useful in testing access to the Operations Manager Management Server.</p>
Alert Routing Rules	<ul style="list-style-type: none"> <li>• Add alert routing rules to specify the Service Manager template that should be used when incidents are created. This is useful because you can use a specific template that is based on the priority or severity of the alert that is generated in Operations Manager. You can also set alert rule criteria, such as the following:           <ul style="list-style-type: none"> <li>• Management Pack Name</li> <li>• Computer for which the alert was raised</li> <li>• Operations Manager class for which the alert was generated.</li> </ul> </li> </ul>
Schedule	<p>Define the poll in seconds that the connector should use when synchronizing alerts. The default is every 30 seconds.</p> <p>You can also decide whether alerts in Operations Manager should be closed when incidents are resolved in Service Manager, and whether incidents should be resolved in Service Manager when alerts in Operations Manager are closed. These two options are very useful.</p> <p>For example, in Operations Manager, if a condition that caused an alert is fixed, Operations Manager automatically closes the alert. By setting these options, you can also configure Service Manager to automatically resolve the associated incident.</p>

After you create the Alert connector, you must finish the configuration by creating a subscription in the Operations Manager Operations console. In the Administration pane of Operations console, Service Manager creates an internal connector named Alert Sync:<ServiceManagerConnectorName>. You can view this in the Internal Connectors view of the Product Connectors node. Edit the connector, and add a subscription that defines the groups, targets, and criteria to use when alerts are forwarded through the connector to Service Manager. This is useful because you can use the criteria to filter alerts. Only the alerts for which you want to generate an incident in Service Manager are forwarded, such as alerts with a Critical severity and a High priority.

### Creating an Operations Manager CI Connector

Use the Operations Manager CI Connector wizard to create a CI connector to Operations Manager. Open the wizard by clicking Create connector in the Tasks pane in Service Manager, which is in the Connectors

node, in the Administration pane of the Service Manager Console. When you create the connector, you must supply several connection settings, which are described in the following table.

Operations Manager CI Connector wizard page	Details
Server Details	<p>Specify the computer name of the Operations Manager Management Server and the credentials that should be used to connect to the computer. The credentials that are specified here are in the form of a Run As account. The account that is used to connect to the Operations Manager Management Server must have the following permissions:</p> <ul style="list-style-type: none"> <li>• Must be a domain account.</li> <li>• Must be a member of the user's local security group on the management server.</li> <li>• Must be a member of the Operators user role in Operations Manager.</li> <li>• Must be a member of the Advanced Operator user role in Service Manager.</li> </ul> <p>A Test connection button is available, which is useful in testing access to the Operations Manager Management Server.</p>
Management Packs	Select the Management Packs that import and reconcile configuration items from Operations Manager. You typically use the Select All option to make sure that all configuration items are imported.
Schedule	On this page, you can configure the schedule that the connector should use when it is running its synchronization. You can configure the schedule to run on a specified day of the week and on a specified hour, such as every Friday at 10:00 P.M.

For more information about how to import Data and Alerts from System Center Operations Manager, go to the following link:

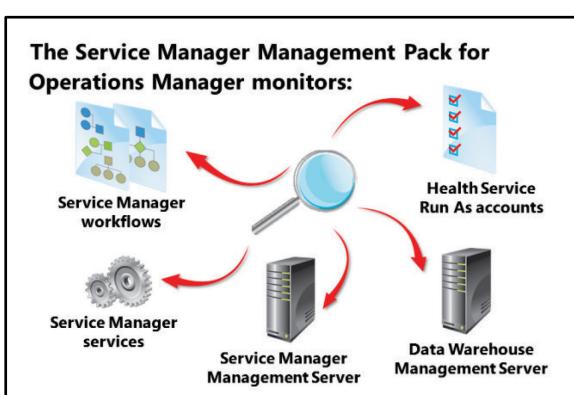
#### Importing Data and Alerts from System Center Operations Manager

<http://go.microsoft.com/fwlink/?LinkId=321905>

## The Process of Monitoring Service Manager with Operations Manager

To enable health and performance monitoring of the Service Manager environment, you should install the Service Manager Management Pack for Operations Manager. This provides additional monitoring of the Service Manager environment, including the following:

- Service Manager services, such as the System Center Configuration Management Service and the System Center Data Access Service
- Health Service Run As accounts
- Service Manager workflows



Both the Data Warehouse Management Server and the Service Manager Management Server are monitored by using the Service Manager Management Pack.

In addition to the Service Manager Management Pack for Operations Manager, it is recommended that you install the following Management Packs to provide comprehensive monitoring for the Service Manager environment:

- Windows Server Operating System
- Windows Internet Information Services
- Microsoft SQL Server
- SharePoint Server

This guarantees that the health, performance, and availability of the Service Manager environment, including the components on which it relies, are monitored effectively.

## Demonstration: Configuring the Operations Manager Alert Connector

In this demonstration, you will learn how to configure the Operations Manager Alert connector.

### Demonstration Steps

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SM1</b>
Tool	<b>Service Manager Console</b>
Pane	<b>Administration</b>
View	<b>Connectors</b>

2. Use the **Create Connector** task to create a new **Operations Manager Alert** connector with the following settings (all other settings should remain default settings):

- Name: **Demo**
- Server Details: **LON-MS1**
- Credentials: **Pa\$\$w0rd**

3. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration\Product Connectors</b>
View	<b>Internal Connectors</b>

4. Edit the properties of the Alert Sync:Demo connector, and add an alert subscription with the following setting (all other settings should remain the default settings):
  - Subscription Name: **Critical Alerts**
5. Stop the WWW service on LON-MS1, and then confirm the **IIS 8 Web Site is unavailable** alert is created in the **Active Alerts** view in the Operations console.

6. Open the alert, and then note the **Ticket ID**.
7. Log on to LON-SM1, and then open the Service Manager Console.
8. From the **Incident Management** node of the **Work Items** pane, open the **All Incidents** view.
9. Confirm an incident was created that has the **Ticket ID** noted earlier.
10. From the **All Windows Computers** view in the **Computers** node of the **Configuration Items** pane, edit the properties of **LON-MS1.CONTOSO.COM**.
11. From the **Related Items** tab, confirm that the incident was added to the **Work items affecting this configuration items** section.
12. Restart the WWW service on LON-MS1.
13. Disable the **Demo** connector on LON-SM1.

**Question:** When you use the Operations Manager Alert connector, you must make sure that only critical alerts are forwarded through the connector from Operations Manager to Service Manager. How can you achieve this?

## Lesson 2

# Data Protection Manager Integration

Protecting business-critical data in any organization is a key function that should be included in the monitoring of the overall IT environment. When backups fail, you need to be notified so that you can diagnose and resolve the issue that caused the failure. The monitoring solution should integrate with the backup solution so that you can view the health of backups, which includes running historic reports that will also be useful in capacity planning.

It is important that you understand how Data Protection Manager integrates with Operations Manager, including how integration is configured and how Data Protection Manager tasks can be performed from within the Operations console.

Finally, to ensure that Data Protection Manager remains in an optimal state, it is important that you understand how you monitor it effectively with Operations Manager via the appropriate Management Pack.

## Lesson Objectives

After completing this lesson, students will be able to:

- Describe System Center 2012 R2 Data Protection Manager.
- Describe the features of integrating Data Protection Manager with Operations Manager.
- Configure Data Protection Manager integration with Operations Manager.

## Overview of Data Protection Manager

Data Protection Manager (DPM) provides data backup and restore functions for the Windows Server and client operating systems. In DPM, a backup is referenced as protection and a restore is referenced as a recovery.

DPM provides intelligent protection and recovery for Microsoft applications, such as the following:

- Hyper-V
- Exchange Server
- SharePoint Server
- SQL Server

### **Data Protection Manager provides:**

- Protection and recovery for Windows servers and clients
- Intelligent protection for Microsoft applications
- Block-level backups
- Disk and tape-based backup
- End-user recovery
- Self-service recovery

For example, when it protects Microsoft SQL Server, DPM can detect new databases and automatically provide protection. DPM provides protection by installing an agent on the computers that must be protected. For computers in the same domain or trusted domain as the DPM server, you can install agents remotely. For computers in untrusted domains or in perimeter networks, you can manually install the DPM agent and attach it to the DPM server. You can use certificates to provide secure authentication between the DPM agent and the DPM server.

When you configure protection for an application, operating system, or file data, you create what is known as a *protection group*. Use a protection group to group similar data types, such as all SQL Server databases or all Exchange Server databases.

When you create a protection group, use the Create New Protection Group Wizard to configure several settings that are specific to that protection group. For example, the following table displays key settings to apply to a protection group that provides protection for all databases running SQL Server:

Create New Protection Group Wizard page	Description
Select Protection Group Type	Specify either servers or clients. Use the Server option to protect file servers or application servers, such as servers running SQL Server or Exchange Server. Use the Clients option to protect desktops and portable computers.
Select Group Members	Select the data that you want to protect. DPM presents a tree view of the computer. This includes any data that it can protect. Use this when you select the data, such as All Volumes, to provide complete protection. DPM also supports Bare Metal Recovery and System State protection. Use this when providing protection for Domain Controllers because it protects and restores AD DS.
Select Data Protection Method	Specify which method should be used to provide protection. You choose short-term protection where DPM stores the protected data on disk, online protection where DPM stores the data in the cloud using Microsoft Azure or tape-based protection where the data is stored on tape.
Select Short-Term Goals	When you select the short-term protection method, you can configure the retention range and synchronization frequency for the protection group. This determines how long data should be retained and how frequently data that was stored by DPM is refreshed to make it consistent.
Review Disk-Allocation	DPM displays the total allocated data size and disk space that DPM will use when it protects the selected data. You can quickly determine how much space is required and adjust the allocated data space, if required.
Choose Replication Creation Method	Specify how DPM should create the replica of the protected data. You can decide to create the replica over the network immediately or schedule it for a later date and time. This is useful when you want to schedule the replica to occur outside working hours so that network performance is not affected.  You can also decide to manually create the replica. Do this when there is a large amount of data to be copied. For example, you can copy the data manually to an external drive, and then copy the data into the DPM storage pool.
Choose Consistency Check Options	On this page, you specify when DPM should check for inconsistencies between the protected data source and the data that is stored in the replica. This is useful because you can have DPM automatically check and fix inconsistencies. This means that the replica is always current. You can also specify a time of day, such as 8:00 P.M., to schedule the consistency checks. This enables you to perform consistency checks outside normal working hours.

When you complete the Create New Protection Group Wizard, DPM creates the protection group and, if you selected it, begins to create a replica of the protected data. DPM uses the Volume Shadow Copy Service (VSS), which enables it to protect data while the data source is online. In addition, after the replica is created, only block-level changes are copied. This reduces data that is stored in the DPM storage pool, and reduces network bandwidth when protecting data.

Use the Recovery wizard to recover data in DPM. Depending on the data that is being recovered, you can select the location for the data recovery. For example, when you recover file data such as a folder, you can decide to recover the folder to its original location or to another location. Do this when you must restore an older version of a file and compare it with a different version. When you recover SQL Server databases, you can decide to recover the database to the original SQL Server or another SQL Server.

Another option that you can select when recovering data is the Restore Security option. You can apply the security settings of the destination computers, or apply the security settings of the data that were applied when the data was protected.

Users can also perform data recovery by using DPM. With End User Recovery, enabled users can recover earlier versions of data by using the shadow copy client. In addition, you can enable Self Service recovery in DPM. This feature provides SQL database owners with the ability to recover databases that they own. When you configure a role in DPM, you configure the domain security groups that can perform recovery of SQL databases and associate them with the instance of SQL Server and database names that they can recover. Then the DPM End User Recovery tool is installed on the computers from which recoveries are performed.

This feature is useful because it enables SQL Server administrators to recover databases that they own without having to access the DPM Administrator Console. The End User Recovery tool provides a similar Recovery wizard that administrators can use to recover databases that they own.

For more information about Data Protection Manager, go to the following link:

#### **Data Protection Manager**

<http://go.microsoft.com/fwlink/?LinkId=321909>

## Features of Integrating DPM with Operations Manager

DPM integrates with Operations Manager by installing the DPM Central Console. With Central Console, you can manage multiple DPM servers and monitor the health and availability of DPM. This includes protection and consistency status for all protected data sources.

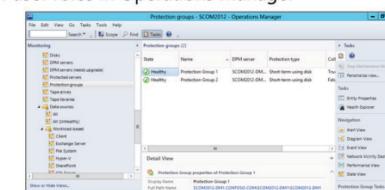
You must import two DPM Management Packs into Operations Manager before you can use the DPM Central Console. Import the following Management Packs from the Management Packs folder on the DPM Media:

- Microsoft.systemCenter.DataProtectionManager.2012.Discovery.mp
- Microsoft.systemCenter.DataProtectionManager.2012.Library.mp

After the Management Packs and the DPM Central Console are installed, several views and tasks become available in the Operations console. You can use these views and tasks to manage and monitor DPM.

### Integrating DPM with Operations Manager provides:

- Monitoring of the DPM environment
- Management of DPM from within Operations Manager
- Management of multiple DPM Servers from one console
- DPM user roles in Operations Manager



Some important views and tasks that are available with the DPM Management Pack are described as follows:

### **Alert Views**

Find the DPM Alert views in the System Center 2012 Data Protection Manager folder of the Monitoring pane in the Operations console. The Alert Views folder displays alert views that relate to backup alerts and infrastructure alerts. The Backup alerts folder contains alert views that relate to disk backups, such as the alerts that affect multiple data sources view or affect single data sources view.

The Infrastructure Alerts folder contains alert views that relate to DPM servers, such as the Disk Infrastructure Alerts view and the Protected Computer Alerts view. These views assess the overall health status of both DPM and the protection status of data sources that are protected by DPM.

### **State Views**

Find DPM state views in the System Center 2012 Data Protection Manager folder of the Monitoring pane in the Operations console. The State views folder contains several state views that you can use to determine the health of many DPM objects, such as the following:

- Disks
- DPM servers
- Protection groups
- Tape drives
- Protected servers

When you select a state view, the health state of the object is displayed in the Details pane. Use views to obtain a quick view of the health state of each DPM component. For example, when you select the DPM Servers State view, the health state of all monitored DPM servers is displayed. When you select a DPM server in this view, several DPM-related tasks become available under the DPM Server Tasks section of the Tasks pane. Other DPM server tasks become available when other views are selected.

### **DPM Server Tasks**

Several DPM server tasks let you manage and operate multiple DPM servers directly from the Operations console. For example, when you select a DPM server in the DPM Servers State view, the Manage DPM Server task opens the DPM Administrator Console for the selected server.

When you select a protection group from the Protection Groups State view, several other DPM tasks become available, such as Run Consistency Check For Protection group and Troubleshoot Protection Group. The Troubleshoot Protection Group task opens a scoped DPM Administrator Console in which alerts generated for the selected protection group are displayed.

Use a combination of views and tasks in Operations Manager to remotely manage, monitor, and maintain all DPM servers from the Operations console.

### **DPM User Roles**

When you manage DPM through the Operations console, you can scope user access in DPM by using the DPM user roles. These roles are configured just as any other Operations Manager user role. Following are examples of DPM user roles:

- **DPM Read-Only Operator.** Lets users view DPM configuration, jobs, and alerts, but prevents users from changing or updating any settings.
- **DPM Tape-Admin.** Lets users perform all tape-related actions.
- **DPM Recovery Operator.** Lets users perform recovery of data that is protected by DPM.

By using DPM user roles, you can distribute relevant DPM tasks to operators in the environment. This is especially useful in large enterprise environments where DPM administration is distributed across multiple DPM owners.

## The Process of Configuring Integration Between DPM and Operations Manager

Before configuring integration between DPM and Operations Manager, you should import the two DPM Management Packs as described at the beginning of the Topic “Features of Integrating DPM with Operations Manager.” In addition, you should deploy an Operations Manager agent to all DPM servers that require monitoring.

Integrate DPM and Operations Manager by selecting the DPM Central Console link in the Data Protection Manager Setup window. This opens the Data Protection Manager Central Console Setup wizard. The following table describes the settings that you configure when you install the DPM Central Console.

To configure integration between DPM and Operations Manager, you must:

1. Import the DPM Management Packs
2. Install an Operations Manager agent on the DPM servers
3. Install the DPM Central Console
  - Install the server-side components
  - Install the client-side components



Data Protection Manager Central Console Setup wizard page	Description
Central Console Opt-In	<p>The Central Console is divided into the following parts:</p> <ul style="list-style-type: none"> <li>• <b>Server-side components.</b> You must install these components on an Operations Manager Management Server.</li> <li>• <b>Client-side components.</b> You must install these components on the computer where the Operations console will be opened.</li> </ul> <p>On this page, you decide whether the server-side or client-side components should be installed, and whether to install both components. This is useful if both the Management Server and Operations console are installed on the same computer.</p>
Prerequisites Check	<p>The wizard checks to make sure that all prerequisites are installed according to the components you selected on the Central Console Opt-In page. If any prerequisites are not met, installation stops and a description and resolution for the prerequisites that failed are displayed.</p>
Installation settings	<p>View the location where the DPM program files will be installed, and view the amount of required and available disk space on the Program Files drive.</p>

As soon as the installation has completed, you can open the DPM Administrator Console by using the desktop icon that is created. When you open the console, you must enter the DPM server name that you want to administer and to which you want to connect. All views and tasks for DPM become available in the Operations console.

For more information about how to install the Central Console, go to the following link:



**Install Central Console**

<http://go.microsoft.com/fwlink/?LinkId=321910>

**Question:** What primary function does the DPM Central Console provide?

## Lesson 3

# Orchestrator Integration

Automating data center processes and tasks is key to delivering a consistent and well-performing IT environment. Additionally, by automating processes and tasks, you alleviate much of the administration overhead in managing them and remove the risk of performance errors. As an example, consider the following scenario.

A known error that occurs periodically on a Windows Server because of a bug in an in-house application generates an alert in the Operations console. Until a fix can be developed for the bug, a manual process of restarting the application service is performed. If this does not fix the problem, a restart of the server is required.

In an environment with no automation capabilities, a manual process of restarting the service and server is required after detection of the problem. This can lead to a number of problems, such as the following:

- It takes too long for the alert to be acted upon, and thus a reduction in service cannot be avoided.
- The wrong service is restarted.
- The wrong server is restarted.
- The processes are not tracked and recorded.

It is important that you understand how Orchestrator is integrated with Operations Manager so that you can provide automation of many tasks in Operations Manager. Finally, to ensure that Orchestrator remains in an optimal state, it is important that you monitor it effectively with Operations Manager via the appropriate Management Pack.

### Lesson Objectives

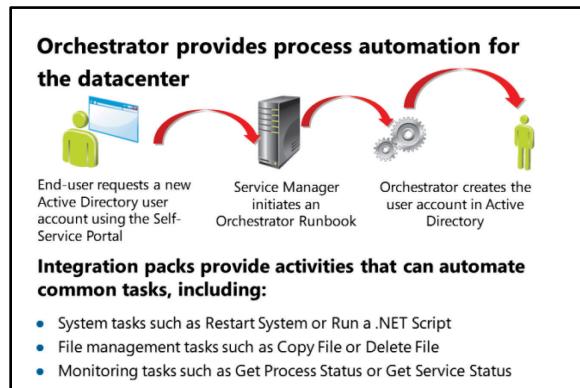
After completing this lesson, students will be able to:

- Describe System Center 2012 R2 Orchestrator.
- Describe how Orchestrator integrates with other System Center 2012 R2 components.
- Describe the Operations Manager Management Pack for Orchestrator functionality and capabilities.

### Overview of Orchestrator

Orchestrator is a process automation solution for the datacenter. Its primary function is to provide a method of automating and managing processes and tasks that are usually performed manually or by using a batch or script file.

Orchestrator integrates with other System Center 2012 R2 components through what is known as *Integration Packs*. Integration Packs provide the links to or activities for an action within the integrated component. For example, when the Integration Pack for Operations Manager is registered and deployed in Orchestrator, you can use an activity named Create Alert to create an alert automatically in Operations Manager. In the same manner, when the Service Manager Integration Pack is registered and deployed, you can use an activity named Create Change With Template to automatically create a change request in Service Manager.



Orchestrator provides Integration Packs for the following System Center 2012 R2 components:

- Configuration Manager
- Data Protection Manager
- Operations Manager
- Service Manager
- Virtual Machine Manager

In addition, there is an Integration Pack for AD DS and several other systems including Exchange, HP, and IBM.

For a list of Integration Packs, including where they can be downloaded from, go to the following link:

 **Integration Packs for System Center 2012 - Orchestrator**

<http://go.microsoft.com/fwlink/?LinkId=321914>

## Activities

In addition to providing integration with other System Center 2012 R2 components, Orchestrator provides several activities that you can use to automate many other tasks. The following table describes some of the activities that Orchestrator provides.

Activity type	Description
System	<p>Includes the following activities:</p> <ul style="list-style-type: none"> <li>• End Process</li> <li>• Query WMI</li> <li>• Restart System</li> <li>• Run .NET Script</li> <li>• Start/Stop Service</li> </ul> <p>For example, you can use the Start/Stop Service Activity to pause, start, stop, or restart a Windows service.</p>
File management	<p>Includes the following activities:</p> <ul style="list-style-type: none"> <li>• Copy File</li> <li>• Delete File</li> <li>• Get File Status</li> <li>• Rename File</li> </ul> <p>Use these activities to manage log files. For example, you can use the Copy File activity to copy a file to a different location. Then you can use the Delete File activity to delete the file from its original location. Use this when you are managing backups where a backup log is archived after a successful backup.</p>
Notification	<p>Includes Send Event Log Message and Send Syslog Message. Use these activities to generate events in remote systems. For example, use the Send Event Log Message to generate a message that has a severity of Error on a Windows-based computer. Operations Manager then detects this error and raises an alert with the relevant information.</p>
Monitoring	<p>Differs from the other activities included when they are used with the</p>

Activity type	Description
	<p>Operations Manager Integration Pack. Activities include the following:</p> <ul style="list-style-type: none"> <li>• Get Process Status</li> <li>• Get Service Status</li> <li>• Get Disk Space Status</li> <li>• Monitor Event Log</li> </ul> <p>Use these activities to monitor for a particular event, such as when disk space is less than a defined percentage. Then you can use the Delete File activity to remove unneeded log files and free up disk space.</p>
Utilities	<p>Includes these activities:</p> <ul style="list-style-type: none"> <li>• Read Text Log</li> <li>• Compare Values</li> <li>• Monitor Counter</li> <li>• Write to Database</li> </ul> <p>Use these activities to perform actions that are based on detected events. For example, you can use the Compare Values activity to compare the result code of a process. Then based on the result, you can use the Write To Database activity to update a database table.</p>

### Runbooks

*Runbooks* in Orchestrator provide a method of grouping and linking activities. For example, a runbook named Backup Database might include all the activities to back up a database, whereas the Restore Database runbook might include all the activities to restore a database.

You can link activities in a runbook. This lets activities share data with other activities. This is one of Orchestrator's most powerful features. By linking activities, you can run other activities that are based on the result to which the activity is linked.

For example, consider the scenario that is described at the beginning of this lesson. An in-house application has a bug that requires restarting a service. In Orchestrator, this process can be automated as follows:

1. A runbook is created in Orchestrator.
2. The Monitor Alert activity is added to the runbook. It is configured to connect to the Operations Manager environment where it detects alerts that match the criteria of the failing application.
3. The Run .NET Script is added to the runbook, and a link between the Monitor Alert and Run .NET Script activity is created.
4. The Run .NET Script is configured by using a Windows PowerShell script that restarts the application service. Included in the script is the NetbiosComputerName variable that is added from the Monitor Alert activity. The NetbiosComputerName variable determines the computer on which the .NET script should run.
5. A variable named Result is added to the Run.NET Script Activity, which is updated by the script. The variable indicates whether the script succeeded or failed.
6. The Restart System activity is added to the runbook and linked to the Run .NET Script activity. The Restart System Activity is configured to restart the system on which the alert was generated by using the NetBiosComputerName variable.
7. The link between Run .NET Script and Restart System is edited. An include filter specifies that data should be passed to the Restart System activity when the .NET script fails.

You can automate and eliminate user intervention in the preceding scenario by using the activities that were listed in the preceding table. In addition, you could expand the runbook to include a Change Request activity that creates a change request in Service Manager. You can add a loop in the activity that waits for change request approval before restarting the application server. Furthermore, you could update the alert in Operations Manager to include notification that the problem was fixed.

For more information about Orchestrator, go to the following link:



### Orchestrator

<http://go.microsoft.com/fwlink/?LinkId=321915>

## The Process of Integrating Orchestrator with Operations Manager

To integrate Orchestrator with Operations Manager, you must perform the following tasks on the computer that is running Orchestrator and hosting the relevant Orchestrator component:

1. On the computer hosting the Orchestrator Deployment Manager, register the Operations Manager Integration Pack.
2. On the computer hosting the Orchestrator Deployment Manager, deploy the Operations Manager Integration Pack.
3. On the computer hosting the Orchestrator Runbook Designer, configure the connection to Operations Manager.

These tasks are further explained in the sections and tables that follow.

**After integrating Orchestrator with Operations Manager, the following activities become available:**

- Create Alert
- Get Alert
- Get Monitor
- Monitor Alert
- Monitor State
- Start Maintenance Mode
- Stop Maintenance Mode
- Update Alert

## Registering the Operations Manager Integration Pack

To register an Integration Pack in Orchestrator, you use the Orchestrator Deployment Manager. The Integration Packs folder in Deployment Manager displays any registered Integration Packs. Right-click this folder and then click the Register IP With The Orchestrator Management Server option. This opens the Integration Pack Registration Wizard. The following table describes each page of the Integration Pack Registration Wizard, including the page settings that you can configure.

Integration Pack Wizard page	Description
Select Integration Packs Or Hotfixes	Add the required Integration Packs or hotfixes that you want to use with Orchestrator. The Integration Pack or hotfix must already have been downloaded and made available on a network share or folder that the Deployment Manager has access to. You can add multiple Integration Packs or hotfixes on this page, but you cannot select multiple files at the same time.
Completing The Integration Pack Wizard	Review the list of Integration Packs and/or hotfixes that will be registered, and optionally click the Back button to make any necessary changes. You then click Finish to register the Integration Packs with Orchestrator. In many cases, such as when registering a System Center Integration Pack, you must accept an End-User License Agreement before the Integration Pack can be registered.

After completing the wizard, the Integration Pack is imported and registered with Orchestrator and is displayed in the Integration Pack folder in Deployment Manager. Details such as the version number are also displayed here, which is useful when you need to ensure you are using the latest version of an Integration Pack.

## Deploying the Operations Manager Integration Pack

To deploy an Integration Pack in Orchestrator, you use the Orchestrator Deployment Manager. The Runbook Designer and Runbook Server folders in Deployment Manager display any deployed Integration Packs. Right-click the Integration Packs folder, and then click the Deploy IP To Runbook Server or Runbook Designer option. This opens the Integration Pack Deployment Wizard. The following table describes each page of the Integration Pack Deployment Wizard, including the settings that you can configure.

Integration Pack Deployment Wizard page	Description
Deploy Integration Packs Or Hotfixes	Select the Integration Packs or hotfixes that you want to deploy to the Runbook Designer or Runbook Server. Only registered Integration Packs and hotfixes are displayed on this page.
Computer Selection Details	Add the computers on which the Orchestrator Runbook Designers and/or runbook servers are hosted on. This determines which computers the Integration Packs or hotfixes will be deployed to.
Installation Configuration	Optionally define a schedule of when the Integration Pack or hotfix will be deployed. This is useful because in most cases, any running runbooks must be stopped before the new Integration Pack is deployed. For this reason, you can schedule the Integration Pack to be deployed outside of working hours so as not to interrupt any unbooks running in a production environment. You can optionally choose to deploy the Integration Pack or hotfix without stopping any running

Integration Pack Deployment Wizard page	Description
	runbooks, but you might need to restart the computer to complete the deployment before the new Integration Pack can be used.
Completing The Integration Pack Deployment Wizard	Review the list of Integration Packs or hotfixes that will be deployed, and optionally click the Back button to make any necessary changes. You then click Finish to deploy the Integration Packs or hotfixes with Orchestrator.

After the deployment has completed, the Integration Packs deployed will be displayed in either the Runbook Designers or Runbook Servers folder in Deployment Manager. Only deployed Integration Packs and hotfixes are displayed in these folders.

### Configuring the Connection to Operations Manager

Before configuring the Operations Manager connector in Orchestrator, you must install the Operations console on each runbook server and Runbook Designer that will be used to connect and integrate with Operations Manager. After installing the Operations console, you should then open the console and configure the connection to the Operation Manager Management Server to ensure that you can view Operations Manager information, such as that provided in the Active Alerts view.

To configure Orchestrators connection to Operations Manager, you click the SC 2012 Operations Manager option on the Options menu in the Runbook Designer. This opens a SC 2012 Operations Manager window, where you can add multiple connections to different Operations Manager environments. When you click the Add button to add a new connection, a Connection window opens where you add the connection details, as described in the following table.

Connection setting	Description
Name	Provide a descriptive name for the connection. If you are configuring connections to multiple Operations Manager environments, you should include details that are environment-specific, for example, OpsMgr_Prod for the production environment or OpsMgr_Dev for the development environment.
Server	Specify the computer name that hosts the Operations Manager Management Server feature. This will be used in the runbook activities to connect to Operations Manager.
Credentials	Specify the credentials such as the domain, user name, and password of an account that has access to the Operations Manager environment. Note that depending on the level of integration required, you might need to use an account that is a member of the Operations Manager Administrators user role.
Monitoring Intervals	Specify the Polling and Reconnect values that should be used when connecting to and updating Orchestrator with Operations Manager activities. By default, both the Polling and Reconnect values are set to 10 seconds.

After you configure the settings for the connection, you can click the Test Connection button to confirm that a connection to the Operations Manager Management Server is successful. If a successful connection is made, a pop-up window with a message stating "Connection successful" is displayed.

With the Operations Manager Integration Pack registered and deployed, and the Operations Manager connection configured in the Runbook Designer, you can then use the Operations Manager Activities that are included with the Integration Pack to start automating tasks in Operations Manager.

Described in the following table are the Orchestrator activities that are included with the Operations Manager Integration Pack:

Operations Manager Integration Pack activity	Description
Create Alert	Provides the ability to create an alert in the Operations Manager console. You can include details such as the description, name, priority, and severity of the alert. This activity is useful when you need to generate an alert for a task or procedure that is not being monitored by Operations Manager, such as a failed file archival or error message in a proprietary log file.
Get Alert	Used to obtain alert information from Operations Manager. This includes details such as the priority and severity, the name and description, and the computer on which the alert was generated. This activity is useful when you need to update other systems with alert details generated by Operations Manager, such as a ticketing system, for example.
Get Monitor	Can be used to obtain the health state of monitors running in the Operations Manager environment. This could then be used, for example, to update an external system, such as a ticketing system, when the health state of a monitor changes to critical.
Monitor Alert	Used to start a runbook when a specific alert has been detected in Operations Manager. This can be useful when there is a number of resolution steps that can be performed based on the alert being generated. For example, you can create a runbook that deletes temporary files and archives log files. This runbook could then be started by a Monitor Alert activity that is run when a Low Disk Space alert generated by Operations Manager is detected.
Monitor State	Used to monitor the health state of an object in Operations Manager. This can then be used to run another activity when a given state has been detected.
Start Maintenance Mode	Used to place a monitored object in Operations Manager into Maintenance Mode. This can be useful when you need to work on a particular object and do not want any alerts generated in Operations Manager during this timeframe.
Stop Maintenance Mode	Used to stop Maintenance Mode on a monitored object in Operations Manager. Use in conjunction with the Start Maintenance Mode activity to resume monitoring of an object after you complete work on it.
Update Alert	Used to update the properties of an alert in Operations Manager. Alert properties that can be updated include the owner, resolution state, and ticket ID. This can be useful when you use an activity to resolve an issue detected by Operations Manager. The Update Alert activity can then be used to automatically resolve the alert.

For more information about System Center 2012 R2 Operations Manager activities, go to the following link:

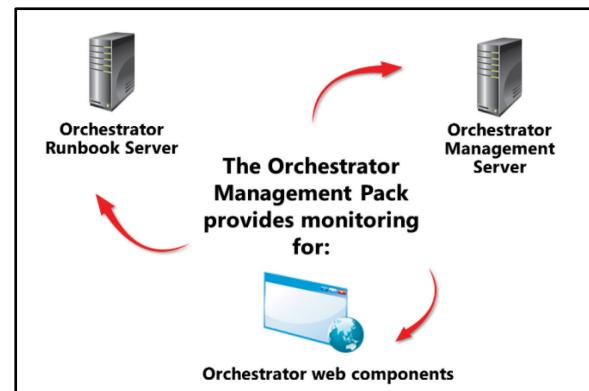
### System Center 2012 Operations Manager Activities

<http://go.microsoft.com/fwlink/?LinkId=391279>

## The Process of Monitoring Orchestrator with Operations Manager

To ensure that the Orchestrator environment is available and performing at optimal levels, you should install the Operations Manager Management Pack for Orchestrator. This Management Pack provides health and availability monitoring of Orchestrator components, including the following:

- Orchestrator Management Server, including the Management Service and database connections
- Orchestrator Runbook Server, including the runbook, remoting services, and database connections
- Orchestrator Web Components, including a health rollup of the Orchestrator web components



After installing the Management Pack, a number of monitoring views become available within the System Center Orchestrator folder in the Monitoring pane of the Operations console. The following list describes each monitoring view:

- **Active Alerts.** Displays any active alerts relating to the Orchestrator environment. This could include alerts relating to failed activities within a runbook or with the Orchestrator components, such as a Management Server or runbook server.
- **Components.** Displays a diagram view of the Orchestrator environment. This includes the Management Servers, runbook servers, and Orchestrator web components. This view is useful in obtaining an up-to-date health state of the overall Orchestrator environment, because the health state of each component is instantly displayed. You can also open other context-sensitive views by right-clicking a component group and then selecting the view such as Alert View, Event View, or Performance View. The Operations Manager Health Explorer for the selected component group can also be opened from here.
- **Management Servers.** Displays the health state of all Orchestrator Management Servers in the environment. Use this view to determine which Management Servers are in a warning or critical health state. You can open other context-sensitive views such as the Alert view, which can then be used to help troubleshoot an unhealthy Management Server.
- **Runbook Servers.** Displays the health state of all Orchestrator Runbook Servers in the environment. Use this view to determine which runbook servers are in a warning or critical health state. You can open other context-sensitive views such as the Alert view, which can then be used to help troubleshoot an unhealthy runbook server.
- **Runbook Targets.** Displays the health state for each runbook target in Orchestrator. Use this view to help troubleshoot failing runbooks by viewing the health state of the runbook's associated target.
- **Web Components.** Displays the health state of the Orchestrator Web console components.

- **Operating System.** Provides a number of operating system performance counters such as available memory, logical disk queue length, and percent processor time. These can be added to the performance dashboard included in this view for the selected Orchestrator computers.
- **PolicyModule Process.** Provides a number of policy module performance counters for the Orchestrator environment, which can then be added to a graph that displays the overall performance over a given period of time.

In addition to the Orchestrator Management Pack for Orchestrator, it is also recommended that you install other relevant Management Packs to monitor the underlying components upon which Orchestrator relies, such as the following:

- Windows Server operating system
- SQL Server
- Microsoft Internet Information Services (IIS)

By using a combination of the Management Packs, you can ensure that your Orchestrator environment remains available, healthy, and performing at optimal levels at all times.

**Question:** You need to automate the creation of an incident record in Service Manager based on an alert generated in Operations Manager. What are the high-level steps that you need to perform to achieve this automation?

# Lab: Configuring System Center Integration

## Scenario

To fully use System Center in the Contoso IT environment, you are asked to integrate Operations Manager with other System Center components, such as Service Manager, Data Protection Manager, Virtual Machine Manager, and Orchestrator. This lets Operations Manager monitor the health and availability of these components. In addition, you are asked to automate the restart of a business-critical website if Operations Manager detects that the website has failed. If the restart of the website fails, Service Manager should create an incident automatically.

## Objectives

After completing this lab, you will be able to:

- Create a connector in Service Manager for Operations Manager and confirm that incidents are created in Service Manager based on alerts generated in Operations Manager.
- Configure integration between Operations Manager and Data Protection Manager.
- Configure Integration between Operations Manager and Orchestrator.
- Use Orchestrator, Operations Manager, and Service Manager to automate a task that restarts a stopped website, and then generates an incident if the restart does not succeed.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machines:** 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-SM1, 10964C-LON-SC1

**User Name:** Contoso\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On LON-HOST1 and LON-HOST2 click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, in Hyper-V Manager, click **10964C-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
  - User Name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:
  - 10964C-LON-SQ1 (On LON-HOST1)
  - 10964C-LON-MS1 (On LON-HOST2)
  - 10964C-LON-SM1 (On HLN-OST2)
  - 10964C-LON-SC1 (On LON-HOST2)



**Note:** Before you start this lab, make sure that all Windows services that are set to start automatically are running, except for the Microsoft .NET Framework NGEN v4.0.30319\_X86 and.NET Framework NGEN v4.0.30319\_X64 services, because these services stop automatically when they are not in use.

## Exercise 1: Configure Service Manager Integration with Operations Manager

### Scenario

To provide integration between Service Manager and Operations Manager, you must configure the Operations Manager Alert connector in Service Manager. When this connector is configured, alerts that are generated in Operations Manager can automatically raise incidents in Service Manager.

The main tasks for this exercise are as follows:

1. Create the Operations Manager connector in Service Manager
2. Configure the Connector in Operations Manager
3. Generate an alert and confirm that an incident is created in Service Manager

### ► Task 1: Create the Operations Manager connector in Service Manager

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SM1</b>
Tool	<b>Service Manager Console</b>
Pane	<b>Administration</b>
View	<b>Connectors</b>

2. Use the **Create Connector** task to create a new **Operations Manager Alert** connector with the following settings (all other settings should remain the default settings):

- Name: **Operations Manager Alerts**
- Server Details: **LON-MS1**
- Credentials: **Pa\$\$w0rd**

### ► Task 2: Configure the Connector in Operations Manager

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration\Product Connectors</b>

Location	Value
View	<b>Internal Connectors</b>

2. Edit the properties of the **Alert Sync:Operations Manager Alerts** connector, and add an alert subscription with the following setting (all other settings should remain the default settings):

- Subscription Name: **Critical Alerts**

► **Task 3: Generate an alert and confirm that an incident is created in Service Manager**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Monitoring</b>
View	<b>Active Alerts</b>

2. Stop the WWW service on LON-MS1, and then confirm the **IIS 8 Web Site Is Unavailable** alert is created in the **Active Alerts** view in the Operations console.
3. Open the alert, and then note the **Ticket ID**.
4. Log on to LON-MS1, and then open the Service Manager Console.
5. Open the **All Incidents** view from the Incident Management node of the **Work Items** pane.
6. Confirm an incident was created that has the **Ticket ID** that was noted earlier.
7. Edit the properties of **LON-MS1.CONTOSO.COM** from the **All Windows Computers** view in the **Computers** node of the **Configuration Items** pane.
8. From the **Related Items** tab, confirm that the incident was added to the **Work items that affect this configuration items** section.
9. Restart the WWW service on LON-MS1.

**Results:** After this exercise, you should have configured the Operations Manager Alert connector in Service Manager and Operations Manager. You should have also tested that the connector works as expected by generating an alert in Operations Manager, and then confirmed that an incident is automatically created in Service Manager. Finally, you should have viewed how Service Manager automatically updates the configuration items with related incidents when they are created in Service Manager.

## Exercise 2: Configure Operations Manager integration with Data Protection Manager

### Scenario

Now that Data Protection Manager is installed, you want to test the monitoring capabilities of Operations Manager when it is integrated with Data Protection Manager. After you configure integration, you also want to protect the Service Manager Database and use Operations Manager to confirm the protection status.

The main tasks for this exercise are as follows:

1. Import the DPM Management Packs
2. Install the DPM Central Console
3. Protect the Service Manager database
4. Verify the protected data in Operations Manager

#### ► Task 1: Import the DPM Management Packs

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration</b>
View	<b>Management Packs</b>

2. Browse to **\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM\Management Packs\en-US**, and copy both Management Packs to the desktop of LON-MS1.
3. Use the **Import Management Packs** task to import both Management Packs.

#### ► Task 2: Install the DPM Central Console

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Setup</b>
Location	<b>\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM</b>

2. Close the **Operations console** if it is open.
3. Install **Microsoft Visual C ++ 2008 Redistributable** by running **vcredist2008\_x64.exe** from the **\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM\Redist\vcredist** folder

4. Install the **DPM Central Console** on LON-MS1 by running **Setup** from the **\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM** folder accepting all default settings.

► **Task 3: Protect the Service Manager database**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>System Center 2012 DPM Administration Console</b>
Pane	<b>Management</b>
Ribbon group	<b>Agents</b>

2. Open the System Center 2012 DPM Administration Console, and then connect to LON-SC1. Use the **Install** option from the **Agents** group to install a DPM agent on LON-SM1 with the following settings (all other settings should remain the default settings):
  - Select agent deployment method: **Install Agents**
  - Select computers: **Add LON-SM1**
  - Enter credentials: **Use the Contoso\Administrator credentials**
  - Restart method: **Select Yes**
3. Wait for the installation to complete.
4. Before you create the **Protection Group**, add the **NT Authority\System** account to the **Sysadmin** server role in SQL Server on **LON-SM1**.
5. In the **DPM Administrator Console** on LON-MS1, from the **Protection** pane, in the **Protection** group, select **New**.
6. Use the **Create New Protection Group Wizard** to create a protection group that has the following settings (all other settings should remain the default):
  - Select group members: Expand LON-SM1 and select the **ServiceManager** database
  - Protection group name: **SQL Server Databases**
7. From the details pane, for the **ServiceManager** database, monitor the **Protection Status** column until the **Protection Status** changes from **Replica creation in progress** to **OK**. This confirms that that the **ServiceManager** database is now protected by DPM.

► **Task 4: Verify the protected data in Operations Manager**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Monitoring\ System Center 2012 R2 Data Protection Manager</b>
View	<b>State Views\DPM Servers</b>

2. Note the **DPM Server Tasks** that are available in the **Tasks** pane when you select **LON-SC1**.
3. Under **State Views**, view the other state views, and then note the data shown in the **Details** pane.

**Results:** After this exercise, you should have configured Operations Manager integration with Data Protection Manager by installing the DPM Central Console. You should have also used the DPM Administration Console from the Operations Manager server to install a protection agent on LON-SM1 and protect the Service Manager database.

## Exercise 3: Configure Orchestrator integration

### Scenario

To automate processes and tasks in the datacenter environment, you must configure integration between Orchestrator, Operations Manager, and Service Manager. This includes importing and registering the relevant Integration Packs in Orchestrator and configuring the connection between Orchestrator, Service Manager, and Operations Manager.

The main tasks for this exercise are as follows:

1. Register and deploy Orchestrator Integration Packs
2. Configure Orchestrator integration with Operations Manager and Service Manager

► **Task 1: Register and deploy Orchestrator Integration Packs**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>Deployment Manager</b>
Folder	<b>Orchestrator Management Server</b>
View	<b>Integration Packs</b>

2. Open the Integration Packs Registration wizard by right-clicking **Integration Packs** and then clicking **Register IP with the Orchestrator Management Server**.
3. Click **Add** on the **Select Integration Packs or Hotfixes** page.

4. Browse To \\LON-DC1\Media\System Center 2012 R2\Orchestrator\Integration Packs, and then add the following Integration Packs:
  - SC2012\_Operations\_Manager\_Integration\_Pack.oip
  - SC2012\_Service\_Manager\_Integration\_Pack.oip
5. Register all Integration Packs, and accept the license agreement for each.
6. Use the **Deploy IP to Runbook Server** or **Runbook Designer** option when right-clicking integration packs to open the **Integration Pack Deployment** wizard:
  - Integration Pack Deployment Wizard: **Select all Integration Packs**
  - Computer selection details: **LON-SC1**
7. Deploy all Integration Packs to LON-SC1, and then close Deployment Manager.

## ► Task 2: Configure Orchestrator integration with Operations Manager and Service Manager

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>Runbook Designer</b>
Menu	<b>Options</b>
Connection to configure	<b>SC 2012 Operations Manager and SC 2012 Service Manager</b>

2. Configure the SC 2012 Operations Manager connection by adding a new configuration with the following settings (all other settings should remain the default settings):
  - Name: **LON-MS1**
  - Domain: **Contoso**
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
3. Test the connection, and then close the **SC 2012 Operations Manager** window.
4. Configure the SC 2012 Service Manager connection by adding a new configuration with the following settings (all other settings should remain the default settings):
  - Name: **LON-SM1**
  - Server name: **LON-SM1**
  - Domain: **Contoso**
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
5. Test the connection, and then close the **SC 2012 Service Manager** window.
6. Close **Runbook Designer**.

**Results:** After this exercise, you should have configured Orchestrator integration with both Service Manager and Operations Manager. This included registering and deploying Orchestrator Integration Packs, installing the Operations Manager Console on the Orchestrator server, and then configuring the Orchestrator connections in the Runbook Designer.

## Exercise 4: Implementing Automatic Website Restart and Creating an Incident if it Fails

### Scenario

To test automatic remediation in System Center 2012 R2, you decide to configure Orchestrator to run a .NET script that restarts the default website on LON-MS1. You also configure the Orchestrator runbook to automatically create an incident in Service Manager when Orchestrator cannot restart the website.

The main tasks for this exercise are as follows:

1. Configure Windows PowerShell for remote operations
2. Import the runbook into Orchestrator
3. Stop the Default Web Site on LON-MS1 and confirm that runbook automatically restarts it
4. Stop and disable the WWW Service and confirm an incident is automatically created by Orchestrator

### ► Task 1: Configure Windows PowerShell for remote operations

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b> <b>LON-MS1</b>
Tool	<b>PowerShell</b>
Cmdlet to Run	<b>Set-ExecutionPolicy unrestricted</b> <b>Enable-psremoting –force</b>

2. Run the **Set-ExecutionPolicy** unrestricted and **Enable-psremoting –force** cmdlets on both LON-SC1 and LON-MS1 computers.
3. Add the **Contoso\Orchestrator\_SVC** account to the **Administrators** local group on LON-MS1.

► **Task 2: Import the runbook into Orchestrator**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>Runbook Designer</b>
Runbook to import	<b>Restart_Website.ois_export</b>
Location	<b>C:</b>

2. Ensure the **Orchestrator Runbook Service** is running.
3. Use the **Import** option from right-clicking **Runbooks** to import the **Runbook**. Use **Pa\$\$w0rd**.
4. Select the **Restart Web Site** runbook, and then from the toolbar, click **Run**.

► **Task 3: Stop the Default Web Site on LON-MS1 and confirm that runbook automatically restarts it**

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Monitoring</b>
View	<b>Active Alerts</b>

2. In IIS Manager on LON-MS1, stop the **Default Web Site**, and then wait for the **IIS 8 Web Site is unavailable** alert to be created in the **Active Alerts** view in the Operations console.

 **Note:** After approximately two minutes, the alert will disappear because Orchestrator has restarted the website. Operation Manager detects this, and then automatically resolves the alert because the condition no longer exists.

3. Confirm that the **Default Web Site** was automatically restarted.

► **Task 4: Stop and disable the WWW Service and confirm an incident is automatically created by Orchestrator**

1. To perform this task, use the computer and tool information that is shown in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Services</b>
Service	<b>World Wide Web Publishing Service</b>

2. Stop and disable the WWW Service.
3. Open the Operations console, and then wait for the **IIS 8 Web Site is unavailable** alert to be created in the **Active Alerts** view.
4. On LON-SM1, open the Service Manager Console, and then confirm the **Failed to restart Web Site** incident was created in the **All Incidents** view, which is in the **Incident Management** node of the **Work Items** pane.
5. Restart the **WWW Service** on LON-MS1.

**Results:** During this exercise, you imported an Orchestrator runbook. The runbook should detect when a default website is unavailable, and then automatically restart it. If the runbook cannot automatically restart the website, the runbook creates an incident in Service Manager. You tested this integration by first stopping the default website on LON-MS1, and then confirming that the website restarted automatically. You then stopped and disabled the WWW service. This made it impossible for the website to be started. Then you confirmed that an incident was automatically created in Service Manager.

**Question:** You have configured the Operations Manager Alert connector in Service Manager, but when alerts are generated in Operations Manager, incidents are not created in Service Manager. What causes this?

**Question:** You have created a runbook in Orchestrator based on an alert from Operations Manager that is used to restart a website automatically. When the website is stopped, the alert is generated, but the Orchestrator runbook does not automatically restart the website. What causes this?

# Module Review and Takeaways



**Best Practice:** You should know how each component of the System Center 2012 R2 product integrates with other components of the product. The System Center 2012 R2 Integration Map from Microsoft provides a map of each System Center 2012 R2 component and displays how each components integration is configured. The System Center 2012 R2 Integration Map can be downloaded from this webpage:  
<http://go.microsoft.com/fwlink/?LinkId=391280>

## Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
When you use the Add Operations Manager wizard in Virtual Machine Manager to integrate Operations Manager and Virtual Machine Manager, you might encounter the following error:  Error 25907 - The credentials used to connect to Operations Managers management group do not have the necessary permissions.	
The script does not execute as expected when you use the Run .NET Script Activity in Orchestrator to run a PowerShell script against a computer that is hosting a Data Protection Manager Server.	

## Review Question(s)

**Question:** You must automate the restart of a Windows service, based on an alert that is generated by Operations Manager, and then automatically generate an incident in Service Manager. What are the minimum System Center 2012 R2 components that are required to make this easier, and how should they be configured to provide this automation?

## Real-world Issues and Scenarios

After you have configured the Operations Manager CI connector in Service Manager, you might find that configuration items are not updated in Service Manager based on objects that were discovered in Operations Manager. This can occur when the relevant Management Packs were not imported into Service Manager.

For objects that were discovered in Operations Manager to be available as configuration items in Service Manager, the same Management Pack that Operations Manager uses to discover these objects must also be imported into Service Manager.

After you import the Management Packs into Service Manager, you must also edit the CI connector and add the Management Packs to be included in the connector's synchronization schedule.

## Tools

Orchestrator Integration Packs for System Center 2012 R2: You can use these Integration Packs to automate many activities in System Center 2012 R2. To download the Integration Packs, go to the following link: <http://go.microsoft.com/fwlink/?LinkId=391280>



# Module 11

## Troubleshooting, Tuning, and Disaster Recovery

### Contents:

Module Overview	11-1
<b>Lesson 1:</b> Troubleshooting and Maintaining Operations Manager Core	
Components	11-3
<b>Lesson 2:</b> Tuning Management Packs	11-18
<b>Lesson 3:</b> Configuring SQL AlwaysOn for Operations Manager	11-24
<b>Lesson 4:</b> Configuring Data Retention in Operations Manager	11-28
<b>Lesson 5:</b> Disaster Recovery in Operations Manager	11-34
<b>Lab:</b> Troubleshooting Operations Manager	11-42
Module Review and Takeaways	11-44

## Module Overview

Your monitoring solution must be highly available to ensure your key line-of-business applications are available and performing at optimum levels at all times. Additionally, ensuring your monitoring solution is fully optimized helps prevent outages and performance deterioration of performance of the monitoring solution. In this module, you will learn how to optimize the data warehouse to ensure the correct volume of data is kept.

As with all key systems, it's important to know where to look when troubleshooting issues. For example, you can use reports to understand performance and know which logs to investigate on both the Management Servers and agents.

To increase overall service availability, you might also consider configuring SQL AlwaysOn for Microsoft System Center 2012 R2 Operations Manager, which increases the availability of the database layer. If a component within the Operations Manager environment fails, it is important that you understand how to recover the failed component.

In this final module of the course, you will learn how to optimize, troubleshoot, and perform disaster recovery in Operations Manager.

### Objectives

After completing this module, students will be able to:

- Troubleshoot Operations Manager core components.
- Tune Management Packs.
- Configure SQL AlwaysOn for Operations Manager.
- Configure data retention for the data warehouse database in Operations Manager.
- Perform disaster recovery in Operations Manager.

## Lesson 1

# Troubleshooting and Maintaining Operations Manager Core Components

Many components make up an Operations Manager Management Group, so it is important that you understand how to troubleshoot each of those components, including which tools you should use and when to use them. You should understand how reporting in Operations Manager can also be used to help troubleshoot the monitoring infrastructure. You should also be aware of the various logs that Operations Manager keeps, including the Operations Manager event log, which is created whenever an Operations Manager component is installed.

## Lesson Objectives

After completing this lesson, students will be able to:

- Troubleshoot Operations Manager by using agent and Management Server logs.
- Troubleshoot agent communication.
- Troubleshoot Operations Manager by using the Operations Manager event Logs.
- Troubleshoot Operations Manager by using reports.

## Agent and Management Server Logs

You can use the Operations Manager logs created on Management Servers and agents to help troubleshoot a number of problems in Operations Manager. For example, if an installation of a Management Server is unsuccessful, you can use the Setup log file and review log entries relating to the installation.

### Management Server Logs

By default, Operations Manager stores log information locally on Management Servers in the C:\Users\<UserName>\AppData\Local\SCOM\LOGS folder. The *UserName* placeholder refers to the user name of the account used when installing Operations Manager. In this folder are a number of logs relating to the various components in Operations Manager are maintained. The following list describes each log:

#### Operations Manager creates the following logs during installation:

- OMConsole.log
- OMServer.log
- OpsMgrSetupWizard.log
- SCOMPreqCheck.log
- WebConsole.log
- SetupX.log
- <computername>AgentInstall.log
- <computername>AgentPatch.log
- <computername>MOMAgentMgmt.log

- **OMConsole.log.** If the Operations console is installed on the Management Server, the OMConsole.log file stores log information during the installation process.
- **OMServer.log.** When installing the Management Server, setup logs information to this log file.
- **OpsMgrSetupWizard.log.** When installing an Operations Manager feature such as a Management Server or the Web console, general log information relating to the activity and progress of the installation is logged in this log file.
- **SCOMPreqCheck.log.** The output from running the prerequisite checker is stored in this log file in .xml format.
- **WebConsole.log.** When installing the Web console, setup stores its log information in this file.

- **SetupX.log**. Each time setup is run on the computer, a detailed SetupX.log file is created. The X placeholder represents a numbered value that is incremented every time setup is run.

### Agent Logs

When an agent is installed on a computer to be managed by Operations Manager, the OpsMgrSetupWizard.log file is created in the C:\Users\<UserName>\AppData\Local\SCOM\LOGS folder and contains information relating to the agent installation. A SetupX.log file is also created that includes detailed information relating to the agent installation.

If the agent was deployed by using the console (push method), additional log files are created in the C:\Program Files\Microsoft System Center 2012 R2\Operations

Manager\Server\AgentManagement\AgentLogs folder on the Management Server that was selected when running the Discovery Wizard. For each agent deployed, the following three log files are created:

- **<computername>AgentInstall.log**. A verbose log of the remote agent installation. The log includes details such as the start time, build version, installer used, and any errors generated during the installation.
- **<computername>AgentPatch.log**. A verbose log of any patches that have been deployed to the agent. This could be cumulative updates that have been applied to Operations Manager, or updates to Management Packs such as the Active Directory helper object.
- **<computername>MOMAgentMgmt.log**. A Windows installer log file that includes log information relating to agent upgrades or agent repairs.

### Enabling debug Trace Logging

Although typically only used when requested by Microsoft, on each computer where an Operation Manager agent, Management Server, or Gateway Server is installed, you can enable trace logging by running **StartTracing.cmd** from a Command Prompt window followed by the level of debugging required. For example, the following command line would enable verbose logging.

```
StartTracing VER
```

There are four possible levels of debug logging:

- **ERR**. Logs error details.
- **WRN**. Logs warning details.
- **VER**. Logs verbose details.
- **INF**. Logs informational details.

To stop debugging, you run the **StopTracing** command, as shown here.

```
StopTracing
```

When enabled, the debug log files are written to the C:\Windows\Logs\OpsMgrTrace folder and are created in .etl format. This format is used by Microsoft Custom Support Services when diagnosing a problem in Operations Manager. You can use the **FormatTracing.cmd** command to convert the .etl log file into a .log format that is viewable in a text editor such as Notepad.exe. To convert the log file to this format, run the following command line.

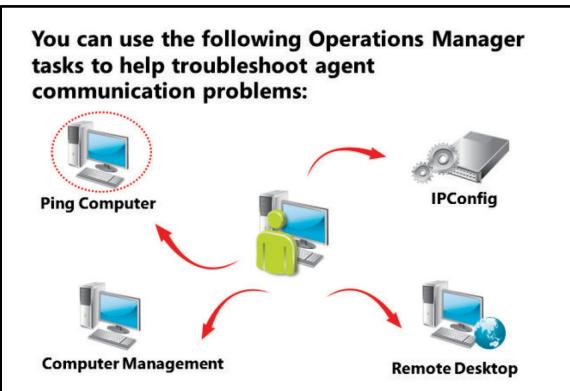
```
FormatTracing
```

The converted log files are created in the C:\Windows\Logs\OpsMgrTrace folder. Depending on the Operation Manager feature you are debugging, the location of the debug logging commands described earlier is different. Use the following table to determine where the commands reside.

Operations Manager feature	Debug commands location
Management Server	C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server\Tools
Gateway Server	C:\Program Files\System Center Operations Manager\Gateway\Tools
Agent	C:\Program Files\Microsoft Monitoring Agent\Tools

## The Process of Troubleshooting Agent Communication

One of the most common troubleshooting tasks performed in Operation Manager is agent communication. If the Management Server loses communication with an agent, a Health Service Heartbeat Failure alert is generated in the Operations console. When this happens the management server will try to ping the agent-managed computer. If ping fails then a second alert is generated. Additionally, the State column for the computer, as shown in the Windows Computers view of the Monitoring pane in the Operations console, is typically unavailable.



To help troubleshoot communication problems between an agent-managed computer and the Management Server the computer reports, to you should first use the tools made available in the Operations console. The Active Alerts view from the Monitoring pane displays any hardware, configuration, application, or operating system errors detected on the agent-managed computer, so this should be one of the first areas to check when troubleshooting. You can then use a number of Operations Manager tasks available in the Operations console to help troubleshoot the problem. The following table describes the tasks that can be used from Tasks pane in the Operations console when a computer is selected in the Windows Computers view in the Monitoring pane.

Operations Manager task	Description
Ping Computer	Use to determine if the computer is connected to the network. When run, a Console Task Output window opens, in which the output generated by running the ping command against the selected computer is displayed. If the results show a successful reply from the ping command, you can be sure there is no network routing issue between the agent and the Management Server.
IPConfig	Use to connect to the selected computer and obtain the IP configuration, and then display the results in a Task Output window. You can use this task to confirm IP settings such as the IP address, subnet mask, and default gateway.
Computer Management	Use to determine if the Windows operating system is responding on the agent-managed computer. You can use the Computer Management task to open Computer Management for the selected computer, where you can then examine components including services, event logs, and Device Manager to help troubleshoot the communications problem.
Remote Desktop	Use to connect remotely to the agent-managed computer and log on as if you

Operations Manager task	Description
	were a local user. You can then investigate the problem locally by using the event logs, services, and any application installed on the computer.

With the exception of the Ping Computer task just described, all tasks will not work in scenarios where the Microsoft Monitoring Agent service is stopped on the agent-managed computer. This is also the case if the agent-managed computer is turned off.

In cases where the tasks described in the preceding table appear to return the expected values, you might need to log on to the agent-managed computer and perform additional troubleshooting:

- **Confirm the Microsoft Monitoring Agent is running.** Open Services, and then confirm the Microsoft Monitoring Agent service is running. If it is not, start the service. If it is running, restart the service.
- **Confirm the agent can connect to the Management Server.** Ping the Management Server from the agent-managed computer.
- **Review the Operations Manager event log. Review the events recorded in the Operations Manager event log on both the agent-managed computer and its assigned Management Server. This is described in detail in the next topic.**
- **Confirm the agent can connect to the Management Server on port 5723.** Do this if possible, and if security policy permits, install the Telnet Client feature on the agent-managed computer, and then from a command prompt, enter the command that follows. If the Command Prompt window is cleared and just a flashing cursor is displayed, a successful connection on port 5723 was made. If a "Could not open connection to the host" message appears, the agent cannot connect to the Management Server and the issue could possibly be a firewall configuration issue or the health service is not running on the management server.

```
telnet <ManagementServerName> 5723
```

- **Delete the Health Service Store cache files on the agent-managed computer.** The agent stores cached Management Pack data, including rules and monitors, in the C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State\Health Service Store folder. You can force the agent to download a fresh copy of these files from the Management Server by performing the following steps:
  1. Stop the Microsoft Monitoring Agent service.
  2. Delete the files in the **C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State\Health Service Store** folder.
  3. Start the Microsoft Monitoring Agent service.
- **Repair the agent.** As a penultimate step in restoring communication between the agent and the Management Server, you can run the Repair task that is available from the Tasks pane when a computer is selected in the Agent Managed view of the Device Management node in the Administration pane of the Operations console. When using the Repair task, you can use the Management Server Action account or specify an account that has local administrative rights on the agent-managed computer. Note that the Repair task is available only for agents that were deployed by using the console. Manually installed agents cannot be repaired by using this task.
- **Remove and reinstall the agent.** If all troubleshooting tasks described earlier in this topic do not resolve the agent communication problem, reinstalling the Operations Manager agent should be performed. You can use the Uninstall task from the Tasks pane to remotely uninstall the agent. The Uninstall task becomes available when you select a computer in the Agent Managed view of the Device Management node in the Administration pane of the Operations console. If the strategy of

using Uninstall fails because of the communication problem, you must uninstall the agent by using Programs And Features in Control Panel on the agent-managed computer. Note that you might need to manually delete the computer from the Agent Managed view in the Operations console if you are removing the agent by using this uninstall method, to ensure the computer is removed from the Operations Manager database. Also note that if the agent is multihomed, you will need to reinstall the agent from each Management Group. To determine which Management Group the agent reports to, you can open the Microsoft Monitoring Agent properties from Control Panel. The Management Group section on the Operations Manager tab displays each Management Group that the agent reports to. You can also use the Add button from this tab to manually add the agent to a Management Group.



**Note:** You can also repair an Operations Manager agent by using the Get-SCOMAgent and Repair-SCOMAgent PowerShell Cmdlets. The following example repairs the agent running on LON-AP1.Contoso.com:

```
Get-SCOMAgent -DNSHostName "LON-AP1.contoso.com" | Repair-SCOMAgent
```

## Reviewing the Operations Manager Event Logs

Operations Manager provides extensive logging for all core components within the Operations Manager event log. This event log can be viewed by opening the Event Viewer on any computer that is hosting an Operations Manager role. In the Event Viewer, the Operations Manager log is located under the Applications and Services Logs folder.

The Operations Manager event log should be one of the first tools you use when troubleshooting any problem with Operations Manager, because a record of almost any event occurring in

Operations Manager is recorded here. For example, if a Management Servers communication with an agent-managed computer is broken, Event ID 20022 is generated in the Operations Manager event log on the Management Server. The description of the event includes the message "The entity <ComputerName> is not heartbeating." Other useful information such as the date and time that the event was logged, and the computer on which the event was logged, are also included in the event.

Depending on the Operations Manager role installed, you can filter the events displayed in the event log by using the Filter Current Log option, which you access by right-clicking the event log. This option helps you filter the log to display the events you are interested in. For example, if you are troubleshooting a reporting problem where data is not appearing in reports, you could filter the Operations Manager event log to display only events with an event source of Operational Data Reporting. You could further filter the event log to display only Critical and Warning events. Filtering events in this way can greatly reduce troubleshooting time because you do not need to scroll events that are not related to the issue you are troubleshooting.

An example of using the Operations Manager event log to troubleshoot an Operations Manager agent communication issue follows.

### The Operations Manager event log can be used to troubleshoot problems by:

- Including a descriptive message of errors detected
- Providing an event ID that can be used when searching knowledge bases
- Providing details of any remote computers the agent cannot connect to such as a Management Server

### Scenario: Using the Operations Manager Event Log to Troubleshoot an Operations Manager Agent Communication Issue

You have deployed an Operations Manager agent to a Windows Server 2012 R2 computer named LON-DC1 that is running in the same domain as the Management Server it is assigned to. You view the Windows Computers view in the Monitoring pane of the Operations console, and note that the computer is displayed and its status is showing as healthy. After approximately 10 minutes, you open the Windows Computers view again and notice that the computer is unavailable. You perform the troubleshooting tasks outlined in the following table.

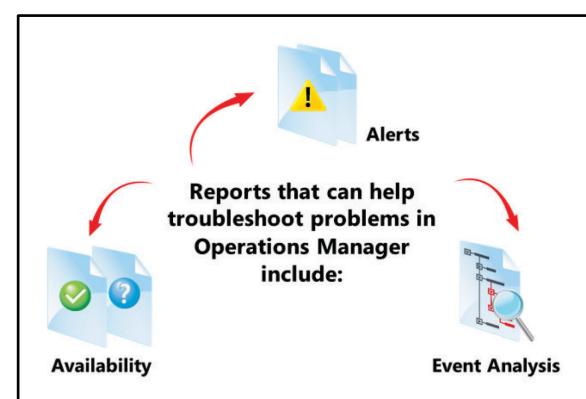
Troubleshooting task performed	Result
Open the Active Alerts view in the Operations console.	A Health Service Heartbeat alert has been generated on the LON-DC1 computer. A Failed To Connect To Computer alert has also been generated.
Run the Ping Computer task in the Operations console.	A successful reply from the IP address of LON-DC1 is displayed.
Review the Operations Manager event log on LON-DC1.	Error event 21006 has been generated with the following event message: "The OpsMgr Connector could not connect to LON-MS1:5723. The error code is 11001L (no such host is known). Please verify network connectivity, the server is running and has registered its listening port, and there are no firewalls blocking traffic to the destination."
Install the Telnet Client feature and run Telnet LON-MS1 5723 on LON-DC1.	You receive a message stating "Could not open connection to the host."

Upon realizing that your environment uses a dedicated Management LAN, you notice that the Ethernet cable connected to the Management LAN has been disconnected. You reconnect the Ethernet cable and then refresh the Operations Manager event log on LON-DC1. Event ID 21019 has been logged with a message stating "OpsMgr has returned to communicating with its primary host LON-MS1.CONTOSO.COM." After a short period of time, the agent's health state returns to healthy in the Operations console.

Reviewing the Operations Manager event log is typically one of the first troubleshooting tasks performed, because it is immediately updated by Operations Manager whenever an issue is detected.

## The Process of Using Reports to Assist with Troubleshooting

In addition to the Operations Manager logs and event logs discussed earlier in this module, you can use reports in Operations Manager to help troubleshoot problems with the core components of Operations Manager. For example, the Alerts report, which you can access in the Microsoft Generic Report Library folder of the Reporting pane, displays all alerts generated by the health service on a Management Server or an agent-managed computer. This report can also be useful in obtaining a historical view of common alerts that have occurred over a period of time. This



information can then be correlated with other events that have occurred in the environment to determine trends.

To generate a report that displays alerts relating to the health service, perform the following steps in the Operations console:

1. In the Operations console, click the **Reporting** pane.
2. Click the **Microsoft Generic Report Library** folder.
3. From the details pane, click **Alerts**.
4. From the **Tasks** pane, click **Open**.
5. In the **Alerts – Operations Manager – Report** window that opens, click **Add Object**.
6. In the **Add Object** window that opens, in the **Search** box, type the computer name, and then click **Search**.
7. Under **Available items**, click the computer name, where the Class column displays **Health Service Watcher**, click **Add**, and then click **OK**.
8. Click the **From** drop-down list, and then click the **From** date (for example, **Yesterday**).
9. Click **Run** to run the report.

Alerts relating to the Health Service Watcher are then displayed in the report. Included in the report are details such as the alert name, repeat count, priority, object, first raised date, and last raised date. You can also expand each alert displayed. Use a linked report named Alert Detail Report to further investigate the selected alert and view other details about it, such as its description and custom fields.

Other reports that can be useful in troubleshooting include:

- **Event Analysis.** The Event Analysis report can be used to display events of specific source, type, and event ID. This report can be useful when you need to determine how widespread a particular issue is. For example, you can include all agent-managed computers in the report and then filter the report based on a known event ID. Computers on which the event occurred within the specified time frame would then be displayed in the report.
- **Availability.** The Availability report can be used to obtain the availability of any monitored object in Operations Manager during a given period of time. You can select which criteria should be included as downtime in the report, such as planned or unplanned maintenance. The report displays the availability of the selected object as a percentage. You can then open an Availability Tracker for the selected object to pinpoint specific areas of time when an object was unavailable. This report can be useful when you need to determine the availability of an agent-managed computer over a given period of time to assess the computer's overall availability.

## Maintaining the Operations Manager Environment

To help maintain the Operations Manager environment, a number of daily, weekly, and monthly tasks should be performed. These tasks will help ensure that your Operations Manager environment is running optimally and (in the event of a disaster) will ensure that the most recent data can be restored. The tables below describe each maintenance task.

### Daily Tasks

#### Maintaining the Operations Manager environment involves:

- Reviewing Management Group Health
- Reviewing Active Alerts
- Taking a back up of the Operations Manager databases
- Running data volume reports
- Updating Management Packs
- Taking a back up of custom Management Packs

Task	Description
Review the health of the Management Group	Use the Operations console to review the overall health of the Management Group. The Management Group Health dashboard provides an at-a-glance view into the health state of each core component in Operations Manager including management servers, agents, and the Operations Manager databases. This dashboard can also be published to SharePoint using the Operations Manager SharePoint Web Part, so it is an ideal web page to display on a large screen where it can be viewed regularly. The dashboard automatically updates every 15 minutes and is opened from the Operations Manager folder in the Monitoring pane of the Operations console.
Review active alerts	Use the Active Alerts view from the Monitoring pane to review any new alerts that have been generated and troubleshoot accordingly. Additionally the Monitoring Overview page can be used to view the overall health state for monitored computers and distributed applications. Click the Monitoring node in the Monitoring pane to view the Monitoring Overview page.
Back up the operational database	Take an incremental back up of the operational database.

### Weekly Tasks

Task	Description
Back up the operational database	Take a full back up of the operational database.
Back up the data warehouse database	Take an incremental back up of the data warehouse database. Depending on your data retention policy you may decide to opt for a full backup instead.
Backup the ACS database	Take an incremental back up of the ACS database. Depending on your data retention policy you may decide to opt for a full backup instead.
Run the Data Volume by Management Pack report	The Data Volume by Management Pack report provides an overview of the data generated by each Management Pack. This includes Alerts, Discoveries, Events, State changes and performance counter instances collected. From this report you can see which management packs are generating the most data. You can then focus tuning on these management packs.
Run the Data	The Data Volume by Workflow and Instance report provides an overview of

Task	Description
Volume by Workflow and Instance report	the data generated by workflows such as monitors, rules and discoveries. Similar to the Data Volume by Management Pack report you can use this report to focus tuning on monitors and rules that are generating the most data.

**Monthly Tasks**

Task	Description
Back up the data warehouse database	Take a full back up of the data warehouse database.
Back up the ACS database	Take a full back up of the ACS database.
Back up bespoke management packs	Back up any custom management packs that you have developed.
Update management packs	Use the <i>Import Management Packs</i> task with the Management Pack Catalog Web Service to check for updated management packs and import as necessary.



**Note:** To assist with managing the backup of bespoke management packs, consider creating a PowerShell script to automate and schedule this process. There are also 3<sup>rd</sup> party management packs available that perform a scheduled backup of unsealed management packs.

**Question:** Where are the Operations Manager setup logs created when you install any Operations Manager component?

## Lesson 2

# Tuning Management Packs

It is important that you know which monitors and rules are included in the management packs you import into Operations Manager. This helps you understand which components (or objects) the management pack monitors and collects data from, and will also help when tuning the management pack.

In this lesson you will learn some of the key management pack tuning techniques to keep the Operations Manager environment running optimally and allow operators to concentrate on monitoring the performance, health and availability of the environment.

### Lesson Objectives

After completing this lesson, students will be able to:

- Use the Operations console to view Management Pack contents.
- Use Overrides and Targeting to tune Management Packs.

## Viewing Management Pack Objects in Operations Manager

As you have learned in previous modules, as soon as a management pack is imported into Operations Manager, it begins immediately discovering and monitoring the objects for which it was designed. With default configuration and threshold settings in each management pack you can quickly and easily start to monitor applications and services without any prior knowledge or expertise. In environments where these applications and services are configured appropriately and running optimally, a management pack may not generate alerts initially since the configuration and monitored thresholds do not breach any of the management pack's default settings. However, if the management pack detects a configuration drift or when an application breaches a threshold, then alerts will start to appear in the Operations console.

**After importing a Management Pack in Operations Manager you can view Management Packs objects such as:**

- Attributes
- Monitors
- Object Discoveries
- Overrides
- Rules
- Tasks
- Views

**Use the Scope and Find Now buttons to search for specific Management Pack objects**

For this reason, it is important that you import management packs on a one-by-one basis allowing time for each management pack to discover all objects that it monitors. Before importing the next management pack you should fine-tune the management pack so that it is customized for your environment. This is important because if you decide to import multiple management packs at the same time, you may get a flood of alerts in the Operations console making it difficult to troubleshoot the root cause of a problem detected by Operations Manager. In addition, this also makes tuning a management pack difficult as you may find that you create override conflicts by adding overrides for the same object on a rule or monitor from different management packs.

### Viewing Management Pack Objects

It should be noted that before importing a management pack you should always read the accompanying management pack guide. The guide provides information about what is monitored by the management pack, any configuration required before or after the management pack is imported and any security related information such as running the management pack in a low-privileged environment.

After importing a management pack most of the objects related to tuning can be found in the Management Pack Objects folder in the Authoring pane of the Operations console. This includes the following:

- *Attributes*. Each class such as the Windows Server 2012 Logical Disk class defined within a management pack has a number of properties associated with it. An *attribute* is a property of a class.
- *Monitors*. Monitors determine the health of a monitored object in Operations Manager.
- *Object Discoveries*. Object Discoveries are used to discover objects that Operations Manager can manage.
- *Overrides*. Overrides are used to change the default monitoring thresholds or values that have been applied to rules, monitors and object discoveries.
- *Rules*. Rules are used to collect data, generate alerts and run commands on agent-managed computers.
- *Tasks*. Tasks are used to run commands or scripts on either agent-managed computers or on computers running the Operations console.
- *Views*. Views are used to display data that has been collected by Operations Manager and includes managed objects. Views are accessed and configured in the Monitoring pane of the Operations console. In this folder however all views for each target class are displayed.

You can use the views listed above to view management pack objects and create overrides on rules, monitors and object discoveries. For example, suppose you wanted to view all of the rules that are included with the Windows Server 2008 Internet Information Services 7 management pack. You can do this by performing the following steps:

1. In the **Operations console**, click the **Authoring** pane.
2. Expand **Management Pack Objects** and then click **Rules**.
3. From the toolbar click **Scope**.
4. In the **Scope Management Pack Objects** window that opens click the **Clear All** button to clear any selections.
5. Click **View all targets**.
6. Click the **Management Pack** column name to sort the objects by management pack.
7. Select the rules in which the **Management Pack** column displays **Windows Server 2008 Internet Information Services 7**.
8. Click **OK**.

The details pane now displays every rule that belongs to the Windows Server 2008 Internet Information Services 7 management pack.

The Scope button as described above is useful when you need to determine which objects are included in a specific management pack. The Scope button can also be used with other objects such as object discoveries, monitors, tasks and attributes.

If you need to find a particular object such as a rule or monitor to create an override, you can also use the *Find Now* button from the toolbar. This lets you search objects by using either the full name or a partial name of the object. For example, suppose you wanted to find the *Logical Disk Free Space* monitor. You can type “*logical*” in the *Look for* box in the toolbar and then click *Find Now*. The list of monitors displayed in the details pane includes those monitors with the word “*logical*” in their name.

Using a combination of the Scope and Find Now buttons you can quickly and easily find management pack objects in Operations Manager.

## Using Overrides and Targeting to tune Management Packs

As mentioned in the previous topic, it is best practice to import management packs on a one-by-one basis allowing time for each management pack to discover and monitor objects that it was designed for. You should also consider importing management packs into a pre-production environment first. This way you can work on tuning the management pack before it is imported into the production environment along with the associated overrides management pack you have created.

### When tuning Management Packs in Operations Manager you can:

- Create unsealed Management Packs to store overrides
- Use Alerts to create Overrides
- Target Overrides at Objects, Classes or Groups
- Enforce parameters in Overrides

In many cases, when planning to tune a management pack you may need to consult the application or service owner to ensure that any overrides applied to objects within the management pack are configured with appropriate values. This is important, as in many cases the Operations Manager operator may not be a subject matter expert in a particular application or service so would not necessarily know the best threshold levels to set on rules or monitors within a management pack.

The easiest and quickest method of tuning a management pack is to review the alerts it generates and then apply overrides to the relevant objects. Using this approach allows you to concentrate on the most important alerts first, such as critical alerts.

You can right-click an alert in the Operations console and then use the Overrides feature to override a rule or monitor associated with the alert. What is useful about creating overrides in this manner is that the overrides feature is context sensitive in most cases. Meaning that the specific object that caused the alert to be generated is made available when creating the override. This allows you to target the rule or monitor directly at the monitored object (if desired) thereby providing a more granular approach to fine-tuning a management pack. To use this feature you select the *For the object* option when creating the override.

When overriding a rule or monitor based on an associated alert, you should determine how the override is to be created. You may need to consider whether to change a monitored threshold or other parameter, or disable the rule or monitor. Keep the following in mind when evaluating alerts to determine how the associated rule or monitor should be overridden:

- *Actionability*. Does the alert provide information that is sufficient for you to resolve the problem detected?
- *Validity*. Is the alert valid based on the problem detected?
- *Alert Suppression*. If there is more than one alert for the same problem, consider configuring alert suppression.

### What should you override?

The answer to what you should override for a given rule, monitor or object discovery will vary depending on your environment and on which object you are applying the override. Consider the following when creating an override:

- *Discovery frequency*. Do you need to change how often Operations Manager checks to discover new objects in the environment?
- *Monitor thresholds*. Do you want to change the threshold of a monitor so that an alert is not generated or the health state is not affected?
- *Targets*. What is the overrides target object?

- *Interval*. Do you want to change how often a specific condition is tested?
- *Parameters*. Do you need to change a specific parameter in a rule, monitor or object discovery to customize it for your environment?

### Using Classes and Groups to target Overrides

When creating an override, irrespective of whether you are creating it from an alert or directly from within the Authoring pane, you must specify the target for the override. The options are as follows:

- *For all objects of class*. Choosing this option will allow you to target the override at the specific class for which the rule or monitor is configured. Note that if an override is being created from an alert, an additional option named *For the object* is made available as described above.
- *For a group*. Choosing this option will allow you to target the override to members of an Operations Manager group. This is useful as you can create a dynamic group that is automatically updated with objects that you want to override. Keep in mind however that in order for the override to use the specified group, the group must be either created in the same management pack as the override or in a sealed management pack.
- *For a specific object of class*. Choosing this option will allow you to target the override at a specified object only. For example, if a rule is targeting a Windows Server 2012 Computer then choosing the *For a specific object of class* option for the override will prompt you to select the specific Windows Server 2012 computer to which the override should be applied.
- *For all objects of another class*. Choosing this option will allow you to apply the override to objects in a class other than the target class.

Note that with the exception of the *For all objects of class* option, the rule or monitor that is being overridden still applies to all other objects within the targeted class. The override changes the settings only for the specified target configured when creating the override. In addition, when moving override management packs between Operations Manager Management Groups, such as from a pre-production environment to a production environment, overrides that target specific objects or groups will not work as expected. This is because objects and groups are reflected as GUIDs which are not available in Management Groups other than those in which the override was created.

### Enforcing Attributes in Overrides

When configuring the settings in an override the *Enforced* attribute can be selected for any parameter. This ensures the setting is applied in the event that another override has been created of the same type where the *Enforced* attribute has not been selected.

You should also keep in mind the following hierarchy when creating overrides:

- Overrides targeting a class are applied first.
- Overrides targeting a group are applied next.
- Overrides targeting an object are applied last.

This means that an override applied to an object will take precedence over an override applied to a class or group.

### Best practices to use when creating Overrides

Depending on how overrides are targeted in Operations Manager, managing them can become a time consuming process. For example, if you always use the *For an object* option when creating overrides to target specific objects you will quickly generate many overrides that will need to be manually maintained and updated as conditions change within the environment. In addition, these overrides are not transferrable to other Management Groups as described earlier. Consider the following order of preference when creating overrides to help manage and maintain them in your environment:

1. If a monitor or rule is not valid for your environment, disable it for the targeted class.
2. If the monitor or rule is valid but the thresholds are not valid for your environment, override it for the targeted class.
3. If the monitor or rule is valid but the thresholds are not valid for a number of objects in your environment, create a dynamic group which dynamically includes these objects and then target the override at the dynamic group.
4. If the monitor or rule is valid but the thresholds are not valid for a specific number of objects in your environment, create a static group which contains these objects and then target the override at the static group.
5. If the monitor or rule is valid but the thresholds are not valid for a specific object, target the override at the specific instance of the targeted class.

Note that when creating overrides using options 4 and 5 above, they will not be transferrable to other Operations Manager Management Groups. For this reason options 1, 2 and 3 should be the preferred method of creating overrides when possible.



**Note:** A useful PowerShell Cmdlet named Get-SCOMOverride can be used to retrieve overrides that have been configured on a set of rules. The following example retrieves all overrides that have been configured for any rules that include the word *disk* in their name:

```
Get-SCOMRule -Name "*disk*" | Get-SCOMOverride -ErrorAction SilentlyContinue
```

## Demonstration: Creating an Override

In this demonstration you will learn how to create an Override in Operations Manager.

### Demonstration Steps

1. To perform this task, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Authoring\Management Pack Objects</b>
View	<b>Rules</b>

2. Use the Scope button to scope the Rules to **Windows Server 2012 R2 Operating System**.
3. Create an Override for the **System Processor Queue Length Windows Server 2012 R2** rule with the following settings:
  - a. Override parameter: **Tolerance**
  - b. Override Value: **5**
  - c. Management Pack: Create a new Management Pack named **Windows Server 2012 R2 OS Overrides**
4. Save the Override.
5. Use the **Overrides Summary** option to confirm the Override has been created.

**Question:** You need to override a parameter for a monitor but only for one server in your environment. The override should not be applied to any other server. What is the best method of doing this?

## Lesson 3

# Configuring SQL AlwaysOn for Operations Manager

The Operations Manager operational database is one of the key components in an Operations Manager Management Group. If the operational database fails or goes offline, almost all functionality in the Management Group is lost. Agents continue to collect monitored data, however, functions performed in the Operations console would not be possible. For this reason, you should understand how Operations Manager can work with SQL AlwaysOn.

## Lesson Objectives

After completing this lesson, students will be able to:

- Describe SQL AlwaysOn.
- Configure SQL AlwaysOn for Operations Manager.

## Overview of SQL AlwaysOn

High availability in Microsoft SQL Server has been available for some time and can be implemented by using a number of different methods, including the following:

- **Failover clustering.** Using a combination of one or more nodes (servers) and two or more shared disks, a *failover cluster* provides high availability for a SQL Server instance. By using what is known as a *resource group*, any one node in the cluster group can make the SQL instance available. If one node fails or becomes unavailable, the resource group automatically fails over to another node in the cluster.
- **Database mirroring.** *Database mirroring* uses a software solution to effectively copy a database between two instances of SQL Server. Typically these SQL instances reside on two separate computers running SQL Server. While one SQL Server instance provides access to one copy of the database, the other SQL Server instance provides a synchronized warm or hot standby to the mirrored database. It should be noted that until the release of SQL AlwaysOn database mirroring was not supported as a high-availability solution for Operations Manager.
- **Log shipping.** *Log shipping* provides a method of backing up transaction logs for a database on a primary SQL Server instance, to one or more databases running on a secondary SQL Server instance. This provides disaster recovery for the database and can also provide read-only access to secondary databases when a primary database is being restored.
- **Replication.** *Replication* provides a method of replicating databases and their associated database objects from one database to another. Data between these databases is then synchronized. There are three replication methods that can be adopted in SQL Server: snapshot, transactional, and merge. For high-availability purposes, and because it provides the lowest latency, the transactional method is typically preferred.

### SQL AlwaysOn provides the following features:

- Uses Windows Server Failover Clustering to provide failover
- Does not require shared storage for Windows Server Failover Clustering
- Uses database mirroring for data transfer
- Provides both synchronous and asynchronous mirroring
- Performs database backups on a replica
- Includes database encryption and compression
- Provides the ability to group databases into availability groups

## SQL AlwaysOn

With the release of SQL Server 2012 is a new feature named AlwaysOn. AlwaysOn uses many of the existing high-availability features available in earlier releases of SQL Server, such as such as database

mirroring, but provides more granular control over high-availability in SQL Server, with less overhead both in terms of infrastructure and administrative effort. Some of the key features of SQL AlwaysOn include the following:

- Uses Windows Server Failover Clustering to provide failover.
- Shared storage for Windows Server Failover Clustering is no longer required.
- Utilizes database mirroring for data transfer.
- Provides both synchronous and asynchronous mirroring.
- Database backups can be performed on a replica.
- Includes database encryption and compression.
- Provides the ability to group databases into availability groups.

To help you understand how AlwaysOn works, the features in the preceding list are described in the following sections.

### **Windows Server Failover Clustering**

Windows Server Failover Clustering is one of the key components of AlwaysOn. It provides the ability to automatically failover resources from one node in a cluster to another node. By monitoring the active node in a cluster, Windows Server Failover Clustering detects when this node has failed and assigns the resources to another node in the cluster. A key point to note is that until now, SQL Server, although cluster-aware, was not able to span multiple subnets. This made utilizing failover clustering over multiple datacenters difficult, if not impossible, for many organizations. With SQL Server 2012, failover clustering can now be configured to work in a multisubnet environment, meaning multisite failover clustering is fully supported.

### **Shared Storage Not Required**

In versions of SQL Server prior to SQL Server 2012, if clustering was required, storage for SQL Server had to be configured as shared storage. This meant clustering SQL Server was typically expensive and time consuming to set up. With SQL Server 2012, you can use a storage area network (SAN), network attached storage (NAS), and direct attached storage (DAS) for Windows Server Failover Clustering, and also use local disk storage.

### **Database Mirroring For Data Transfer**

AlwaysOn uses database mirroring to synchronize databases between one SQL Server instance and another. These database instances and their associated databases can reside on the same server, on different servers, or even in different datacenters. Database mirroring, however, cannot determine which databases are dependent on other databases, meaning that when a failover occurs, the reason could be that a dependent database has not been failed over, resulting in an application failure. AlwaysOn resolves this dependency issue with an availability group, which is described later in this lesson.

### **Synchronous and Asynchronous Mirroring**

AlwaysOn supports both synchronous and asynchronous database mirroring, and even a combination of both. Synchronous mirroring incurs the highest latency but also offers the best protection of data, because that data is written to both the primary and any secondary databases at the same time. Asynchronous mirroring provides the quickest mirroring, because it does not have to wait for any secondary database updates to complete before moving on. This faster mirroring, however, could lead to potential data loss, so depending on your environment, you might need to configure both synchronous and asynchronous database mirroring to reflect your high-availability and disaster recovery needs.

### **Database Backup on a Replica**

AlwaysOn provides the ability to perform maintenance tasks, such as database backup and database snapshots, against secondary replicas. This removes the overhead of running backups and snapshots

against the primary database, thereby keeping the primary database performing optimally and available at all times.

### **Database Encryption and Compression**

To cope with the high bandwidth requirements and relevant security risks when moving large amounts of data during mirroring, backup compression and Transparent Data Encryption tools are employed with AlwaysOn.

### **Availability Groups**

AlwaysOn provides the ability to group databases into what are known as *availability groups*. Using availability groups allows you to group similar or dependent databases together so that they all failover at the same time in the event of a failure on the host server. Availability groups remove the dependency issue noted earlier in the description of database mirroring, because you can ensure all related databases are included within the same group.

### **Creating an SQL AlwaysOn Availability Group**

The following high-level tasks must be performed in SQL Server to create an AlwaysOn availability group:

1. On each server running SQL Server that will be included in the availability group as a replica, install the Failover Clustering feature.
2. Create a cluster, and then include the relevant nodes, cluster name, and virtual IP address.
3. Configure the cluster quorum.
4. In SQL Server Configuration Manager, edit the properties of the SQL Server instance, and on the **AlwaysOn High Availability** tab, select the **Enable AlwaysOn Availability Groups** check box.
5. Restart the SQL Server service.
6. In SQL Server Management Studio, expand **AlwaysOn High Availability**.
7. Right-click **Availability Groups**, and then click **New Availability Group Wizard**.
8. Select the databases that should be included in the availability group. Note that each database must have at least one full backup taken and must be configured for the full database recovery model.
9. Configure the replicas. This involves adding SQL Server instances as replicas, configuring the endpoints, choosing a backup preference such as prefer secondary, secondary only, primary, and any replica. You also configure the listener information such as the Domain Name System (DNS) name, IP address, and port. The listener is the connection point for all clients using the database.
10. Configure the initial data synchronization. You can choose a **Full** data synchronization, or if you already restored a backup to each secondary server, you can choose **Join** instead.
11. Validate the settings for the new availability group, and then click **Finish** to create the availability group.

## The Process of Configuring Operations Manager with SQL AlwaysOn

For System Center 2012 R2, SQL AlwaysOn is supported for the following databases:

- Operational database
- Data warehouse database
- Audit Collection Services (ACS) databases

The configuration steps required to configure Operations Manager and SQL AlwaysOn differ depending on whether you are installing a new Operations Manager Management Group or you are configuring an existing Operations Manager Management Group database for SQL AlwaysOn.

The following high-level tasks describe the steps required in both of these scenarios.

### **Configuring Operations Manager to work with SQL AlwaysOn includes:**

- Creating a new availability group
- Adding availability group replicas
- Configuring the availability group listener
- Backing up the Operations Manager databases
- Adding the Operations Manager databases to the new availability group

### **Configuring a New Operations Manager Management Group to Support SQL AlwaysOn**

If you are installing a new Operations Manager Management Group and want to include support for SQL AlwaysOn, perform the following high-level steps:

1. Create a new availability group by using the **New Availability Group** option in SQL Server Management Studio.
2. Add the availability replicas to the availability group.
3. Create an availability group listener for the availability group, making a note of the DNS name, port, and IP address, if applicable.
4. Install the first Management Server in the Operations Manager Management Group. When prompted to identify which computer hosting the SQL Server you will use, specify the **Group Listener Name** and **Port** specified when creating the group listener in step 3.
5. In SQL Server Management Studio, edit the properties of the OperationsManager and OperationsManagerDW databases, and then change the recovery model of the databases to **Full**.
6. Take full backup of both databases.
7. Add the OperationsManager and OperationsManagerDW databases to the availability group in SQL Server Management Studio. Ensure that the data synchronization option is set to **Full**.
8. On the computer hosting the OperationsManager database, open SQL Server Management Studio and add a logon for the Operations Manager Data Writer account, as specified when installing Operations Manager.
9. On the computer hosting the OperationsManager database, open SQL Server Management Studio, and add a logon for the Management Server action account, as specified when installing Operations Manager.
10. On the computer hosting the OperationsManager database, open SQL Server Management Studio, and add a logon for the Management Server computer account, and then add the following user mappings for the OperationsManager database:
  - **ConfigService**
  - **db\_accessadmin**
  - **db\_datareader**
  - **db\_datawriter**

- **db\_ddladmin**
  - **db\_securityadmin**
  - **sdk\_users**
  - **sql\_dependency\_subscriber**
11. On the computer hosting the OperationsManagerDW database, open SQL Server Management Studio, and then add a logon for the Operations Manager Data Writer account, as specified when installing Operations Manager.
  12. On the computer hosting the OperationsManagerDW database, open SQL Server Management Studio, and then add a logon for the Operations Manager Data Reader account, as specified when installing Operations Manager.
  13. On the computer hosting the OperationsManager database, open SQL Server Management Studio, add a logon for the Management Server computer account, and then add the following user mappings for the OperationsManager database:
    - **db\_datareader**
    - **OpsMgrReader**
    - **apm\_datareader**

#### **Configuring an Existing Operations Manager Management Group to Support SQL AlwaysOn**

If you already have an existing Operations Manager Management Group and want to include support for SQL AlwaysOn, perform the following high-level steps:

1. Create a new availability group by using the **New Availability Group** option in SQL Server Management Studio.
2. Add the availability replicas to the availability group.
3. Create an availability group listener for the availability group, making a note of the DNS Name, Port, and IP address, if applicable.
4. In SQL Server Management Studio, edit the properties of the OperationsManager and OperationsManagerDW databases, and then change the recovery model of the databases to **Full**.
5. On each Management Server in the Management Group, use the Registry Editor to edit the following key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\Database
```

6. Update the **DatabaseServerName** value to **AvailabilityGroupListnerName,portNumber**
7. On each Management Server, edit the following file.

```
%ProgramFiles%\System Center 2012\Operations Manager\Server\ConfigService.config
```

8. In the **<Category>** tag named **Cmdb**, change the value for **ServerName** to the name of the availability group listener, and change the **PortNumber** to the availability group listener port.
9. Update the Operations Manager database with the group listener name and port by following these steps:
  1. Open SQL Server Management Studio.
  2. Expand **Databases\Operations Manager\Tables**.
  3. Right-click **dbo.MT\_Microsoft\$SystemCenter\$ManagementGroup**, and then click **Edit Top 200 Rows**.

4. Change the value in the **SQLServerName\_<GUID>** column to reflect the *<name,port>* of the availability group listener.
5. Save the change.
6. Update the Operations Manager database with the availability group listener to specify the location of the application performance monitoring tables:
  1. Open SQL Server Management Studio.
  2. Expand **Databases\Operations Manager\Tables**.
  3. Right-click **dbo.MT\_Microsoft\$SystemCenter\$OpsMgrDB\$AppMonitoring**, and then click **Edit Top 200 Rows**.
  4. Change the value in the **MainDatabaseServerName\_<GUID>** column to reflect *<name,port>* of the availability group listener and its port.
  5. Save the change.
  6. Right-click each database, and under **Task**, select **Back up (Full Back up)**.
  7. Go to the availability group node and expand it. Right-click **Availability database**, and select **Add database**.
  8. On the **Select Initial Data Synchronization** page, select **Full**. At the end of this task, all databases will be added to the availability database, and restored on all availability replica nodes.
  9. For each of the secondary replicas, open **build\_mom\_db\_admin.sql** in Notepad. The file is located in *<installationMediaFolder>\Setup\AMD64*. Then search for the MOMv3 messages section. Copy this section into SQL Server Management Studio, and then start and run a new query.

For more information about Operations Manager and SQL Server 2012 Always On Availability Groups visit the following website.

 **Using SQL Server 2012 Always On Availability Groups with System Center 2012 SP1 - Operations Manager**

<http://go.microsoft.com/fwlink/?LinkId=404094>

**Question:** What databases in Operations Manager can use SQL AlwaysOn?

## Lesson 4

# Configuring Data Retention in Operations Manager

Both the operational and data warehouse databases can become full over time, so it is important that you configure the data retention settings appropriately for them.

For the operational database, you can configure data retention from within the Operations console. However, you cannot configure data retention in this way for the data warehouse database, so it is important that you understand how to achieve this.

### Lesson Objectives

After completing this lesson, students will be able to:

- Describe the data warehouse retention settings in Operations Manager.
- Configure the data warehouse retention settings in Operations Manager.

### Data Warehouse Retention Settings

As described in the topic titled “Configuring Operations Manager Default Settings” in Module 2 of this course, “Deploying a New System Center 2012 R2 Operations Manager Management Group,” the data retention settings for the Operations Managers operational database can be configured in the Operations console. Data retention for the data warehouse database, however, cannot. You must either use SQL Management Studio to query the database or use the Data Warehouse Data Retention Policy (Dwdatarp.exe) tool provided by Microsoft.

**Data retention settings for the Data Warehouse database can be viewed by using:**

**Data Warehouse Data Retention Policy Tool (Dwdatarp.exe)**



**SQL Server Management Studio**



Data is automatically groomed from the data warehouse database just as it is from the operational database, but as you might expect, because of the need for reporting and capacity planning, data is retained for a much longer period of time in the data warehouse database.

Depending on your data retention policy and your business requirements, it is important that you understand how to view and edit the data retention settings for the data warehouse database. For example, organizations that operate in the payment card industry might have a requirement to keep security related data for long periods of time in the case of a forensic investigation.

Data in the data warehouse database is aggregated as raw data on an hourly and daily basis. The following table includes some of the data types that are aggregated in the data warehouse, including the default data retention settings for each.

Data warehouse data set	Aggregation type	Days retained
Alert	Raw data	400
State	Hourly aggregations	400
Perf	Daily aggregations	400
Event	Raw data	100

### Viewing Data Warehouse Data Retention Settings

To view the data retention settings of the data warehouse database, you can use SQL Server Management Studio as described in the following procedure:

1. Open SQL Server Management Studio, and then connect to the database engine that hosts the OperationsManagerDW database.
2. Expand **Databases**, right-click the **OperationsManagerDW** database, and then click **New Query**.
3. In the query window that opens, type the following.

```
SELECT GroomStoredProcName, MaxDataAgeDays FROM StandardDatasetAggregation
```

4. Click the **Execute** button to execute the query.

The results from the query will show each data set, including the current data retention setting in days.

## The Process of Configuring Data Retention for the Data Warehouse Database

There are two methods of configuring data retention for the data warehouse database in Operations Manager. You can use SQL Server Management Studio, or you can use the Data Warehouse Data Retention Policy (Dwdatarp.exe) tool. Each method is described in the following sections.

### Using SQL Server Management Studio to Configure Data Retention

To configure data retention for the data warehouse database by using SQL Server Management Studio, perform the following steps:

1. In SQL Server Management Studio, connect to the database engine that hosts the Operations Manager DW database.
2. Expand **Databases**, expand **OperationsManagerDW**, and then expand **Tables**.
3. Open the **dbo.Dataset** table.
4. Make a note of the GUID in the **DatasetID** column for the data set that you want to update the groom setting for.

#### You can use the DWDatarp.exe tool to:

**View** the data retention settings for the data warehouse database



**Configure** the data retention settings for the data warehouse database



5. Open the **dbo.StandardDatasetAggregation** table.
6. In the **DatasetID** column, locate the GUID that you noted in step 4.
7. In the **AggregationTypeID** column, locate the aggregation type, scroll to the **MaxDataAgeDays** column, and then update the value with the new grooming value.

You can also use an SQL query to update the data retention settings. For example, the following SQL query, when executed against the OperationsManagerDW database, will change the data retention settings for the AlertGroom dataset from 400 days to 100 days.

```
USE OperationsManagerDW
UPDATE StandardDatasetAggregation
SET MaxDataAgeDays = 100
WHERE GroomStoredProcName = 'AlertGroom'
```

### Using the Dwdatarp.exe Tool to Configure Data Retention

The Dwdatarp.exe tool was developed for Operations Manager 2007 R2. It can be used to view and update the data retention settings for the data warehouse database in both Operations Manager 2007 R2 and all versions of System Center 2012 R2 Operations Manager. To view and set the data warehouse settings by using the Dwdatarp.exe tool, you perform the following sets of steps.

To view data warehouse retention settings:

1. Copy the Dwdatarp.exe tool to a computer that has access to the OperationsManagerDW database.
2. Open a Command Prompt window, and go to the folder where the Dwdatarp.exe tool is located.
3. Enter the following command to view the data warehouse retention settings, replacing <DWservername> with the computer name of the computer hosting the SQL Server for the data warehouse database, and <DWdatabase> with the name of the data warehouse database.

```
dwdatarp.exe -s <DWservername> -d <DWdatabase>
```

For example, the following command displays the data retention setting for the OperationsManagerDW database on LON-SQ1.

```
Dwdatarp.exe -s LON-SQ1 -d OperationsManagerDW
```

To update the data retention settings:

1. Use the Dwdatarp.exe tool to determine the data set name that you want to update.
2. From a Command Prompt window, enter the following command.

```
Dwdatarp.exe -s <DWservername> -d <DWdatabase> -ds <dataset name> -a <aggregation name> -m <days>
```

Replace the parameters enclosed in angle brackets (<>) as follows:

- <**DWservername**>. Computer name of the computer hosting SQL Server
- <**DWdatabase**>. Data warehouse database name
- <**data set name**>. Name of the data set to update
- <**aggregation name**>. Aggregation type
- <**days**>. Number, in days, to change the retention to

For example, the following command update the Event data set data retention to 150:

```
Dwdatarp.exe -s LON-SQ1 -d OperationsManagerDW -ds "Event data set" -a "Raw data" -m
150
```

You can use the Dwdatarp.exe command again to confirm the data retention settings have been updated correctly as described in the first example.

**Question:** What are the two methods that can be used to update the data warehouse data retention settings?

## Lesson 5

# Disaster Recovery in Operations Manager

You need to understand how to recover If components within a Management Group fail. For example if one Management Server fails another Management Server in the Management Group will take over the monitoring that the failed Management Server was providing whilst you recover it. However, If all Management Servers in a Management Group fail then monitored data will be held in the agent cache running on the managed computer but no data will be inserted into the Operations Manager databases.

You should understand the various recovery methods used to recover from a disaster in Operations Manager, including recovering Management Servers and the Operations Manager databases.

## Lesson Objectives

After completing this lesson, students will be able to:

- Recover from a failed Management Server in Operations Manager.
- Recover from a failed operational or data warehouse database in Operations Manager.
- Recover from a failed Web console server in Operations Manager.

## The Process of Recovering a failed Management Server

When multiple Management Servers are deployed in a Management Group, if one Management Server fails, agent communication is automatically distributed to other Management Servers in the All Management Servers resource pool. If all Management Servers fail, however, agent communication is lost, and access to the Operations console is also lost. Agents will continue to monitor, but instead of communicating performance and alert data to their associated Management Server, they will store information locally until communication is restored. Thus, it is important that you understand how to recover from a failed Management Server.

**When recovering a failed Management Server, you must do the following:**

- Build a new server with the same computer name as the failed Management Server
- Run Operations Manager Setup.exe with the /recover switch
- If all Management Servers in the Management Group have been recovered, reconfigure the Run As accounts

If a computer hosting a Management Server fails, you can recover it by using Setup.exe from a command prompt and specify the /recover switch. In cases where all Management Servers in a Management Group fail, you must also reconfigure the Run As accounts. If at least one operational Management Server is operational, you should not reconfigure the Run As accounts. Follow these high-level steps to recover a failed Management Server:

1. Build a new server, and ensure the same computer name as the failed Management Server is used.
2. If necessary, recover the Operations Manager databases from the most appropriate backup.
3. From an Administrative command prompt, run the following command by using the same credentials, Management Group, and database names that were used for the failed Management Server.

```
Setup.exe /silent /AcceptEndUserLicenseAgreement:1 /recover
/EnableErrorReporting:[Never|Queued|Always]
/SendCEIPReports:[0|1] /UseMicrosoftUpdate:[0|1]
/DatabaseName:<OperationalDatabaseName>
/SqlServerInstance:<server\instance> /DWDatabaseName:<DWDatabaseName>
```

```
/DWSqlServerInstance:<server\instance> /UseLocalSystemDASAccount
/DatareaderUser:<domain\username>
/DatareaderPassword:<password> /DataWriterUser:<domain\username>
/DataWriterPassword:<password> /ActionAccountUser:<domain\username>
/ActionAccountPassword:<password>
```

4. Repeat steps 1–3 for each Management Server to be recovered.

In scenarios where all Management Servers have failed, you must also reconfigure the Run As accounts for the Management Group after recovering each Management Server. To reconfigure the Run As accounts, you perform the following high-level steps:

1. Open the Operations console, and then click the **Administration** pane.
2. Expand **Run As Configuration**, and then click **Accounts**.
3. Right-click a **Run As Account**, and then click **Properties**.
4. On the **Credential** tab of the **Properties** window, enter the appropriate credentials.
5. Repeat steps 1–4 for each Run As account.

## The Process of Recovering a failed Operational or Data Warehouse Database

If the operational database becomes corrupt or fails as a result of a hardware or software issue on the computer hosting it, all access to Operations Manager will be lost. In this case the management server caches data until its cache is full. Then as in the case of a failed Management Server, agents will continue to collect performance and monitoring data, but no data will be inserted into the operational database. In the event of a data warehouse database failure, Operations Manager will continue to function, but reporting features will be unavailable.

### Disaster recovery options for the Operations Manager databases include:

- Restoring the operational database
- Restoring the data warehouse database
- Moving the operational database
- Moving the data warehouse database

### Restoring the Operational or Data Warehouse Database

To recover from a failed operational or data warehouse database, you can perform a database restore by using SQL Server Management Studio, as described in the following steps:

1. Open SQL Management Studio on the computer hosting the operational or data warehouse database.
2. Connect to the database engine.
3. In the object explorer pane, right-click **Databases**, and then click **Restore Database**.
4. In the **Restore Database** window that opens, click **Device**, and then click the **ellipsis** button (...).
5. Add the database backup file.
6. Click **OK** to perform the restore.

### Moving the Operational Database to a New Instance of SQL Server

In cases where the operational database must be moved (or restored) to a new computer hosting SQL Server, there are a number of steps that must be taken to update the Management Group for the new

SQL Server instance. The following high-level steps explain how to move the operational database to a new SQL Server instance:

1. Stop all Operations Manager services on all Management Servers in the Management Group.
2. Back up the operational database, and copy the backup file to the new SQL Server instance.
3. In SQL Server Management Studio on the new SQL Server instance, restore the operational database.
4. On each Management Server in the Management Group, update the **DatabaseServerName** key in the registry from the following location.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\Database

5. On each Management Server, edit the **ConfigService.config** file from %ProgramFiles%\System Center 2012\Operations Manager\Server\, and edit the **ServerName** value to be the new SQL Server instance name.
6. In SQL Server Management Studio on the new SQL Server instance, edit the **dbo.MT\_Microsoft\$SystemCenter\$ManagementGroup** table from the OperationsManager database, and change the value in the **SQLServerName\_6B1D1BE8\_EBB4\_B425\_08DC\_2385C5930B04** column to reflect the name of the new SQL Server instance.
7. In SQL Server Management Studio on the new SQL Server instance, edit the **dbo.MT\_Microsoft\$SystemCenter\$OpsMgrDB\$AppMonitoring** table from the OperationsManager database, and then change the value in the **MainDatabaseServerName\_5C00C79B\_6B71\_6EEE\_4ADE\_80C11F84527A** column to reflect the name of the new SQL Server instance.
8. In SQL Server Management Studio, on the new SQL Server instance, add a logon for the Management Server Action account and the Data Reader account.
9. In SQL Server Management Studio, on the new SQL Server instance, add a logon for DAS computer account, and then enable the following mappings in the OperationsManager database:
  - o **ConfigService**
  - o **db\_accessadmin**
  - o **db\_datareader**
  - o **db\_datawriter**
  - o **db\_ddladmin**
  - o **db\_securityadmin**
  - o **sdk\_users**
  - o **sql\_dependency\_subscriber**
10. Open a new query window for the OperationsManager database, and then execute the following SQL commands:
  - o **sp\_configure 'show advanced options',1**
  - o **reconfigure**
  - o **sp\_configure 'clr enabled',1**
  - o **reconfigure**
11. Execute the following query:

- **SELECT is\_broker\_enabled FROM sys.databases WHERE name='OperationsManager'**
12. If the result from running the query in step 11 was the **\_broker\_enabled** value of **1**, do not perform step 13.
  13. Run the following SQL queries:
    - **ALTER DATABASE OperationsManager SET SINGLE\_USER WITH ROLLBACK IMMEDIATE**
    - **ALTER DATABASE OperationsManager SET ENABLE\_BROKER**
    - **ALTER DATABASE OperationsManager SET MULTI\_USER**
  14. Restart the Operations Manager services on all Management Servers in the Management Group.

#### **Moving the Data Warehouse Database to a New Instance of SQL Server**

In cases where the data warehouse database must be moved (or restored) to a new computer hosting SQL Server, steps that must be taken to update the Management Group and Reporting Server for the new SQL Server instance. The following high-level steps describe how to move the data warehouse database to a new SQL Server instance:

1. Stop all Operations Manager services on all Management Servers in the Management Group.
2. Back up the OperationsManagerDW database, and then copy the backup file to the new SQL Server instance.
3. In SQL Server Management Studio on the new SQL Server instance, restore the OperationsManagerDW database.
4. On the computer that hosts the Operations Manager Reporting component, update the **DWDBInstance** key in the registry with the computer name of the new SQL Server instance from the following location.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Reporting

5. On each Management Server, edit the **ConfigService.config** file from **%ProgramFiles%\System Center 2012\Operations Manager\Server\**, and then edit the **ServerName** value to be the new SQL Server instance name.
6. On the Reporting Server component, start the System Center Data Access Service.
7. On the Reporting Server component, go to **http://localhost/reports**, and then edit the connection string for the Data Warehouse Main data source to reflect the new SQL Server instance.
8. On the Reporting Server component, go to **http://localhost/reports**, and then edit the connection string for the **Application Monitoring\NET Monitoring\AppMonitoringSource** data source to reflect the new SQL Server instance.
9. In SQL Server Management Studio on the SQL Server instance that hosts the OperationsManager database, edit the **dbo.MT\_Microsoft\$SystemCenter\$DataWarehouse** table from the OperationsManager, and change the value in the **MainDatabaseServerName\_2C77AA48\_DB0A\_5D69\_F8FF\_20E48F3AED0F** column to reflect the name of the new SQL Server instance.
10. In SQL Server Management Studio on the SQL Server instance that hosts the OperationsManager database, edit the **dbo.MT\_Microsoft\$SystemCenter\$DataWarehouse\$AppMonitoring** table from the OperationsManager database, and change the value in the **MainDatabaseServerName\_5C00C79B\_6B71\_6EEE\_4ADE\_80C11F84527A** column to reflect the name of the new SQL Server instance.

11. In SQL Server Management Studio on the SQL Server instance that hosts the OperationsManagerDW database, edit the **dbo.MemberDatabase** table from the OperationsManagerDW database, and change the value in the **ServerName** column to reflect the name of the new SQL Server instance.
12. In SQL Server Management Studio on the SQL Server instance that hosts the OperationsManagerDW database, add a new logon for the Data Writer account and the Data Reader account.
13. In SQL Server Management Studio on the SQL Server instance that hosts the OperationsManagerDW database, add a new logon for computer account that hosts the Data Access Service, and then include the following mappings:
  - **db\_datareader**
  - **OpsMgrReader**
  - **apm\_datareader**
14. Restart the Operations Manager services on all Management Servers in the Management Group.

## The Process of Recovering from a Failed Operations Console, Web Console, or Reporting Server

No specific recovery process exists when a Web console, Operations console, or Reporting server component fails. Instead you must reinstall these components. Because these components do not hold any Operations Manager data nor affect the key monitoring capabilities, reinstalling them does not present a major issue.

If you must reinstall the Web console, and you want to install a Management Server component on the same computer as the Web console, both the Web console and the Management Server component must be installed at the same time, or the Management Server should be installed first. If you install the Web console first, you cannot then install a Management Server on the same computer. Also note that if you need to access reports from the Web console, the Web console must be installed on the same computer as the Reporting Server component.

When reinstalling these features, you follow the same procedure you used to perform for the initial installation. No additional configuration is required.

**In the event of a disaster, the following Operations Manager components cannot be recovered and must be reinstalled:**



## Demonstration: Recovering the OperationsManager Database

In this demonstration, you will learn how to recover the OperationsManager database.

### Demonstration Steps

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>SQL Server Management Studio</b>
Pane	<b>Object Explorer</b>
Action	<b>Back Up</b>

2. Close the Operations console on LON-MS1 if it is already open.
3. Using **SQL Server Management Studio** on **LON-SC1**, connect to LON-SQ1 and back up the **OperationsManager** database.
4. Using SQL Server Management Studio, delete the **OperationsManager** database.
  - o Clear the **Delete backup and restore history information for databases** check box.
  - o Select the **Close existing connections** check box.
5. On LON-MS1, open the Operations console.
6. On the **Connecting to Server** process, notice that the **Microsoft System Center 2012 R2 Operations Manager** window freezes.
7. Using Task Manager, end the **Microsoft.EnterpriseManagement.Monitoring.Console.exe** process.
8. On LON-SC1, use **SQL Server Management Studio** to connect to LON-SQ1 and then restore the **OperationsManager** database from the **C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup** folder.
9. Restart the **System Center Data Access Service** and **System Center Management Configuration** services on LON-MS1.
10. Open the Operations console, and confirm that the console opens as expected.

**Question:** In what recovery scenario do you need to reconfigure the Run As accounts in Operations Manager?

# Lab: Troubleshooting Operations Manager

## Scenario

You are attempting to install an Operations Manager agent on a Windows Server 2008 R2 computer that hosts a line-of-business application. During the installation, however, an error is reported in the Operations console and the agent fails to install. You need to troubleshoot why the installation failed and fix the problem so that the line-of-business application can be monitored by Operations Manager. In addition, your IT manager has requested that you test the disaster recovery plan to confirm that it is sufficient to recover from both a Management Server failure and a failure of the operational database.

## Objectives

After completing this lab, students will be able to:

- Troubleshoot an agent installation failure in Operations Manager.
- Recover from a Management Server failure.
- Recover from an operational database failure.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machines:** 10964C-LON-DC1, 10964C-LON-SQ1, 10964C-LON-MS1, 10964C-LON-MS2, 10964C-LON-SC1

**User Name:** Contoso\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must make sure that the virtual machines are running by completing the following steps:

1. On both LON-HOST1 and LON-HOST2, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. On LON-HOST1, in Hyper-V Manager, click **10964C-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Contoso**
5. Repeat steps 2 through 4 for the following virtual machines:
  - 10964C-LON-SQ1 (On LON-HOST1)
  - 10964C-LON-MS1 (On LON-HOST2)
  - 10964C-LON-MS2 (On LON-HOST1)
  - 10964C-LON-SC1 (On LON-HOST2)



**Note:** Before you start this lab, make sure that all Windows services that are set to start automatically are running except for the Microsoft .NET Framework NGEN v4.0.30319\_X86

and.NET Framework NGEN v4.0.30319\_X64 services. These services stop automatically when they are not being used.

## Exercise 1: Troubleshooting an Agent Installation Failure in Operations Manager

### Scenario

To troubleshoot the agent installation failure, you must view the task output log in the Operations console to determine the cause of the failure. You should then resolve the problem and install the agent so that the line-of-business application can be monitored by Operations Manager.

The main tasks for this exercise are as follows:

1. Uninstall the Operations Manager agent from LON-DC1
2. Attempt to install the agent on LON-DC1
3. Fix the problem on LON-DC1
4. Install the Operations Manager agent on LON-DC1

### ► Task 1: Uninstall the Operations Manager agent from LON-DC1

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration</b>
View	<b>Device Management\Agent Managed</b>

2. Use the Uninstall task to uninstall the Operations Manager agent from LON-DC1.

### ► Task 2: Attempt to install the agent on LON-DC1

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration</b>
View	<b>Device Management\Agent Managed</b>

2. Attempt to install an agent on LON-DC1 by using the Computer and Device Management Wizard.
3. On the **Auto or Advanced** page ensure **LON-MS1.CONTOSO.COM** is selected under the **Management Server** section.

4. On the **Administrator Account** page, ensure the **Use selected Management Server Action Account** check box is selected.
5. Review the **Task Output** information, and note the **Access is denied** message.

► **Task 3: Fix the problem on LON-DC1**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-DC1</b>
Tool	<b>Active Directory Users and Computers</b>
Group	<b>Administrators</b>
Account	<b>Svc_SCOM2012_msaa</b>

2. In **Active Directory Users and Computers**, add the **svc\_SCOM2012\_msaa** group to the **Builtin Administrators** group.

► **Task 4: Install the Operations Manager agent on LON-DC1**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations Console</b>
Pane	<b>Administration</b>
View	<b>Device Management\Agent Managed</b>

2. Attempt to install an agent on LON-DC1 by using the **Computer and Device Management Wizard**.
3. On the **Auto or Advanced** page, ensure **LON-MS1.CONTOSO.COM** is selected under the **Management Server** section.
4. On the **Administrator Account** page, ensure the **Use selected Management Server Action Account** check box is selected.
5. Review the **Task Output** information, and note the **The task completed successfully** message.

**Results:** After this exercise, you should have reviewed the task output log in the Operations console to determine the cause of the agent installation failure. You should have then resolved the problem that caused the installation failure and successfully installed the Operations Manager agent.

## Exercise 2: Recovering from a Management Server Failure

### Scenario

Although you have a comprehensive disaster recovery plan for Operations Manager, it has never been tested. Your IT manager has asked that you test disaster recovery in the development environment. You should test the recovery of a failed Management Server.

The main tasks for this exercise are as follows:

1. Build a new Management Server
2. Recover the Management Server
3. Confirm the new Management Server is operating

#### ► Task 1: Build a new Management Server

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-HOST1</b>
Tool	<b>Hyper-V Manager</b>
Virtual Machine	<b>LON-MS2_New</b>
Action	<b>Start</b>

2. Shut down LON-MS2 to simulate a Management Server failure.
3. Create a new Virtual Machine named LON-MS2\_New with the following settings (all other settings should remain as default):
  - Name: **LON-MS2\_New**
  - Memory: **1024**
  - Networking: **External Network**
  - Hard Disk: Use the **Attach a virtual hard disk later** option.
4. Edit the settings of the Virtual Machine and add a new hard disk with the following settings (all other settings should remain as default):
  - Disk Format: **VHD**
  - Disk Type: **Differencing**
  - Name: **LON-MS2\_New.vhd**
  - Parent Disk: **Base14A-WS12R2.vhd** from <DriveLetter>:\Program Files\Microsoft Learning\Base
5. In Hyper-V Manager, start LON-MS2\_New, and complete the setup of Windows Server 2012 R2, setting the **Administrator** password to **Pa\$\$w0rd**.
6. Configure the following settings:
  - Computer name: **LON-MS2**
  - IP Address: **10.10.0.65**

- Subnet mask: **255.0.0.0**
  - Default Gateway: **10.10.0.1**
  - DNS Server: **10.10.0.10**
  - Domain: **Contoso.com**
7. Log on to LON-MS2\_New by using the **Contoso\Administrator** account.
  8. Add the **SCOM2012\_Admins** group to the local **Administrators** group.
  9. Log off LON-MS2\_New.

### ► Task 2: Recover the Management Server

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-HOST1</b>
Tool	<b>Hyper-V Manager</b>
Virtual Machine	<b>LON-MS2_New</b>
Action	<b>Start</b>

2. Log on to LON-MS2\_New, and then map a network drive to **\\\\LON-DC1\\Media**.
3. From a command prompt, go to **Z:\\SCOM2012R2**.
4. Type the following, and then press Enter on the keyboard.

```
Setup.exe /silent /AcceptEndUserLicenseAgreement /recover /EnableErrorReporting:Never
/SendCEIPReports:0 /UseMicrosoftUpdate:0 /DatabaseName:OperationsManager
/SqlServerInstance:LON-SQ1 /DWDatabaseName:OperationsManagerDW
/DWSqlServerInstance:LON-SQ1 /DASAccountUser:Contoso\svc_SCOM2012_das
/DASAccountPassword: Pa$$w0rd /DatareaderUser:Contoso\svc_SCOM2012_dwread
/DatareaderPassword:Pa$$w0rd /DataWriterUser:Contoso\svc_SCOM2012_dwwrite
/DataWriterPassword:Pa$$w0rd
/ActionAccountUser:Contoso\svc_SCOM2012_msaa
/ActionAccountPassword:Pa$$w0rd
```

5. Open Task Manager, click **More Details** and then click the **Details** tab.
6. Monitor the **Setup.exe** process, and wait for it to disappear.

### ► Task 3: Confirm the new Management Server is operating

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations console</b>
Pane	<b>Administration</b>

Location	Value
View	<b>Device Management\Management Servers</b>

- From the details pane, confirm **LON-MS2** is displayed and the **Health State** column displays **Healthy**.

**Results:** After this exercise, you should have built a new virtual machine running Windows Server 2012 and joined it to the Contoso network. You then install the Operations Manager Management Server feature by using the Recover switch. Finally, you confirm the Management Group is operational by using the Operations console.

## Exercise 3: Recovering from an operational database failure

### Scenario

As part of your disaster recovery test, you need to recover the operational database and ensure the Management Group continues to function as expected. SQL Server Management Studio is no longer functioning on LON-SQ1 which hosts the operational databases, consequently so you must use another SQL Server to recover the operational database.

The main tasks for this exercise are as follows:

- Back up the OperationsManager database
- Delete the OperationsManager database
- Restore the OperationsManager database
- Confirm the Management Group is operating as expected

#### ► Task 1: Back up the OperationsManager database

- To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>SQL Server Management Studio</b>
Pane	<b>Object Explorer</b>
Action	<b>Back Up</b>

- Close the Operations console on LON-MS1 if it is already open.
- Using SQL Server Management Studio on LON-SC1, connect to LON-SQ1 and then back up the **OperationsManager** database.

► **Task 2: Delete the OperationsManager database**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>SQL Server Management Studio</b>
Pane	<b>Object Explorer</b>
Action	<b>Delete</b>

2. Using **SQL Server Management Studio** on **LON-SC1** connect to **LON-SQ1** and delete the **OperationsManager** database.
  - o Clear the **Delete backup and restore history information for databases** check box
  - o Select the **Close existing connections** check box
3. On LON-MS1 open the **Operations console**
4. Notice the **Microsoft System Center 2012 R2 Operations Manager** window freezes on the **Connecting to Server** process
5. Using **Task Manager** end the **Microsoft.EnterpriseManagement.Monitoring.Console.exe** process

► **Task 3: Restore the OperationsManager database**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-SC1</b>
Tool	<b>SQL Server Management Studio</b>
Pane	<b>Object Explorer</b>
Action	<b>Restore</b>

2. Using **SQL Server Management Studio** on **LON-SC1**, connect to **LON-SQ1** and restore the **OperationsManager** database from the **C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup** folder.

► **Task 4: Confirm the Management Group is operating as expected**

1. To perform this step, use the computer and tool information in the following table.

Location	Value
Computer	<b>LON-MS1</b>
Tool	<b>Operations console</b>
Pane	<b>Monitoring</b>
View	<b>Active Alerts</b>

2. Restart the System Center Data Access Service and System Center Management Configuration services on LON-MS1
3. Open the Operations console, and confirm the Operations console opens as expected.

**Results:** After this exercise, you should have backed up OperationsManager database. You should then have deleted the OperationsManager database, which simulates a database failure. You should then have restored the OperationsManager database. Finally, using the Operations console, you should have confirmed that the Operations Manager Management Group is functional.

**Question:** When installing a Management Server in a disaster recovery scenario, what switch must you use when running Setup.exe?

# Module Review and Takeaways

When troubleshooting Operations Manager 2012 R2 you should also review the Operations Manager TechNet forum. This can be found at the following website:  
<http://go.microsoft.com/fwlink/?LinkId=404095>

## Review Question(s)

**Question:** In a disaster recovery scenario, what Operations Manager components must be reinstalled instead of recovered?

## Real-world Issues and Scenarios

After failover has occurred in an Operations Manager environment that is using SQL Server AlwaysOn, you might receive the following message when opening the Operations Manager console:

"Execution of user code in the .NET Framework is disabled. Enable "clr enabled" configuration option. Could not use view or function 'dbo.fn\_ModuleTypeView' because of binding errors."

To resolve this issue, execute the following SQL query against the database of the new primary replica SQL instance.

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'clr enabled', 1;
GO
RECONFIGURE;
GO
```

## Tools

### Data Warehouse Data Retention Policy (Dwdatarp.exe) tool

The Data Warehouse Data Retention Policy (Dwdatarp.exe) tool can be used to view and update the data retention settings in the data warehouse database. To download the tool, go to the following website:  
<http://go.microsoft.com/fwlink/?LinkId=391283>

## Course Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the course evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

### Course Evaluation

- Your evaluation of this course will help Microsoft understand the quality of your learning experience.
- Please work with your training provider to access the course evaluation form.
- Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

## Module 1: Overview and Architecture

# Lab: Using the System Center 2012 Operations Manager Sizing Helper Tool

### Exercise 1: Calculating the Hardware Requirements for Contoso's Management Group

► Task 1: Configure the standard deployment values

1. Log on to LON-MS1, and then from drive C, double-click **System Center 2012 Operations Manager Sizing Helper Tool v1.xls**.
  2. In the **System Center 2012 Operations Manager Sizing Helper Tool v1.xls** window that opens, click **Close** on the **Microsoft Office Activation Wizard**.
  3. On the **Scenarios** tab, under **Getting Started**, click **Supported Configuration**.
  4. Review the **Supported Configuration**, and then click **Back to Scenarios**.
  5. Click **Best Practices**.
  6. Review the **Best Practices** information, and then click **Back to Scenarios**.
  7. Under **Standard Deployment**, click **Windows Computers Network Devices Application Performance Monitoring**.
  8. Click the \* **Application Performance Monitoring (APM)** drop-down list, and then click **Enabled**.
  9. Click **Submit**.
  10. In the **Scenario: 3000 Windows Computers, 700 APM-enabled Windows Computers and 500 Network Devices** window that opens, scroll down, and in the **Number of Server Computers** box, type **400** in both the **DB Size** and **DW Size** sections.
  11. In both the **DB Size** and **DW Size** sections, in the **Number of APM-enabled Computers** box, type **50**.
  12. In both the **DB Size** and **DW Size** sections, in the **Number of Network Devices** box, type **120**.
  13. Review the **Minimum Hardware Recommendation** information, including the recalculated **DB Size** and **DW Size** values.
  14. Click **Back to Scenarios**.
- Task 2: Review the advanced deployment values
1. In the **System Center 2012 Operations Manager Sizing Helper Tool v1.xls** window, on the **Scenarios** tab, under **Advanced Deployment**, click **Gateway Server**.
  2. Review the **Gateway Server** information, and then click **Back to Scenarios**.
  3. Click **UNIX or Linux Monitoring**.
  4. Review the **UNIX or Linux** information, and then click **Back to Scenarios**.
  5. Click **URL Monitoring**.
  6. Review the **URL Monitoring** information, and then click **Back to Scenarios**.

► **Task 3: Configure the advanced database sizing values**

1. In the **System Center 2012 Operations Manager Sizing Helper Tool v1.xls** window, on the **Scenarios** tab, under **Advanced Database Sizing**, click **DB Size Calculator**.
2. In the **Number of Server Computers** box, type **400**.
3. In the **Number of Network Devices** box, type **120**.
4. In the **Number of APM-enabled Computers** box, type **50**.
5. Note the **Total Size (GB)** value and **DB Estimated Random IO Per Second for Maximum Load Configuration [80% Write, 20% Read]** information.
6. Note the value in the **Estimated IOPS** column for **1-500** agents.
7. Click **Back to Scenarios**.
8. Click **DW Size Calculator**.
9. In the **Number of Server Computers** box, type **400**.
10. In the **Number of Network Devices** box, type **120**.
11. In the **Number of APM-enabled Computers** box, type **50**.
12. Note the **Total Size (GB)** value and **DW Estimated Random IO Per Second for Maximum Load Configuration [80% Write, 20% Read]** information.
13. Note the value in the **Estimated IOPS** column for **1-500** agents.
14. Click **Back to Scenarios**.
15. Click **DB DW Disk Calculator**.
16. In the **Enter Estimated IOPS [From DBSize & DWSize TAB]** box, type **750**.
17. In the **Enter Estimated Disk Space in GB [From DBSize & DWSize TAB]** box, type **434.94**.
18. Review the Estimated # of RAID disks required information, and then click **Back to Scenarios**.
19. Close the **System Center 2012 Operations Manager Sizing Helper Tool v1.xls** window and in the **Microsoft Excel** window that opens click **Save**.

**Results:** After this exercise, you should have configured the System Center 2012 Operations Manager Sizing Helper tool with appropriate values to determine the hardware required for the Contoso Management Group.

## Exercise 2: Creating a Visio Diagram of the Proposed Management Group Design

### ► Task 1: Import the Visio diagram

1. Log on to LON-MS1, and then navigate to the C drive.
2. Double-click **Contoso Management Group.vsdx**, to open the Contoso Management Group Visio diagram.
3. Click **Close** on the **Microsoft Office Activation Wizard**.
4. Review the various Operations Manager components that have been added to the diagram.

### ► Task 2: Include communication flow and TCP/IP ports

1. Click the **Home** tab, and then on the ribbon, in the **Tools** group, click **Connector**.
2. Click and hold the left mouse button on the left **Management Server** shape, and then drag a connector to the **Operational database SQL Cluster** shape, releasing the mouse button to create the connector.
3. Right-click the connector, and then click **Edit Text**.
4. Type **1433** in the box, and then click anywhere in the canvas to save the text.
5. Using the method described in step 2, create a connector from the right **Management Server** shape to the **Operational database SQL Cluster** shape.
6. Right-click the connector, and then click **Edit Text**.
7. Type **1433** in the box, and then click anywhere in the canvas to save the text.
8. Create a connector from the left **Management Server** shape to the **Data Warehouse and SSRS databases** shape.
9. Right-click the connector, and then click **Edit Text**.
10. Type **1433** in the box, and then click anywhere in the canvas to save the text.
11. Create a connector from the right **Management Server** shape to the **Data Warehouse and SSRS databases** shape.
12. Right-click the connector, and then click **Edit Text**.
13. Type **1433** in the box and then click anywhere in the canvas to save the text.
14. Create a connector from the **Reporting Server** shape to the left and right **Management Server** shapes.
15. Right-click the connector, and then click **Edit Text**.
16. Type **5723/5724** in the box, and then click anywhere in the canvas to save the text.
17. Create a connector from the **Web Console Server** shape to both **Management Server** shapes.
18. Right-click the connector, and then click **Edit Text**.
19. Type **5724** in the box, and then click anywhere in the canvas to save the text.
20. Create a connector from the **Web Console** shape to the **Web Console Server** shape.
21. Right-click the connector, and then click **Edit Text**.
22. Type **80** in the box, and then click anywhere in the canvas to save the text.
23. Create a connector from the **Operations Console** shape to both **Management Server** shapes.

24. Right-click the connector, and then click **Edit Text**.
25. Type **5724** in the box and then click anywhere in the canvas to save the text.
26. Create a connector from the top **Agent Managed Computers** shape to both **Management Server** shapes.
27. Right-click the connector, and then click **Edit Text**.
28. Type **5723** in the box, and then click anywhere in the canvas to save the text.
29. Create a connector between the bottom **Agent Managed Computers** shape to the **Gateway Server** shape.
30. Right-click the connector, and then click **Edit Text**.
31. Type **5723** in the box, and then click anywhere in the canvas to save the text.
32. Create a connector from the **Gateway Server** shape to both **Management Server** shapes.
33. Right-click the connector, and then click **Edit Text**.
34. Type **5723** in the box, and then click anywhere in the canvas to save the text.
35. Rearrange the shapes so that all text is visible in the canvas.

**Results:** After this exercise, you should have created a Visio diagram of the proposed Management Group design for Contoso.

## Module 2: Deploying a New System Center 2012 R2 Operations Manager Management Group

# Lab: Installing System Center 2012 R2 Operations Manager and Deploying Agents

### Exercise 1: Installing a New System Center 2012 R2 Operations Manager Management Group

#### ► Task 1: Install the first Management Server

1. Log on to LON-MS1.
2. Browse to \\LON-DC1\Media, and then open the **SCOM2012R2** folder.
3. Double-click **Setup.exe** to start **Operations Manager** setup.
4. In the **Microsoft System Center 2012 R2** window that opens, click **Install**.
5. In the **Operations Manager Setup** wizard, on the **Select features to install** page, select **Management server** and **Operations console**, and then click **Next**.
6. On the Select installation location page, click **Next**.
7. On the **The Setup wizard cannot continue** page, notice that the **Report Viewer controls** are not installed.
8. Browse to \\LON-DC1\Media, and then double-click **ReportViewer.msi**.
9. In the **Open File – Security Warning** window that opens, click **Run**.
10. On the opening page of the **Microsoft Report Viewer 2012 Runtime** wizard that starts, click **Next**.
11. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
12. On the **Ready to Install the Program** page click **Install**.
13. On the **Completing the Microsoft Report Viewer 2012 Runtime Installation** page, click **Finish**.
14. Go back to the **Operations Manager Setup** wizard, and then click **Verify Prerequisites Again**.
15. On the **Proceed with Setup** page, click **Next**.
16. On the **Specify an Installation option** page, in the **Management group name** box, type **SCOM2012**, and then click **Next**.
17. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
18. On the **Configure the operational database** page, in the **Server name and instance name** box, type **LON-SQ1**, press the Tab key on the keyboard, and then click **Next**.
19. On the **Configure the Data Warehouse database** page, in the **Server name and instance name** box, type **LON-SQ1**, press the Tab key on the keyboard, and then click **Next**.
20. On the **Configure Operations Manager accounts** page, type the following details, and then click **Next**.
  - **Primary account:** LON-MS1\scmadmin
  - **Primary password:** Pa55w0rd
  - **Primary account must change password at next logon:**
  - **Secondary account:** LON-MS1\scmadmin
  - **Secondary password:** Pa55w0rd
  - **Secondary account must change password at next logon:**

Account Name	Domain\User Name	Password
Management Server action account	<b>Contoso\svc_SCOM2012_msaa</b>	<b>Pa\$\$w0rd</b>
System Center Configuration service and System Center Data Access service	<b>Contoso\svc_SCOM2012_das</b>	<b>Pa\$\$w0rd</b>
Data Reader account	<b>Contoso\svc_SCOM2012_dwread</b>	<b>Pa\$\$w0rd</b>
Data Writer account	<b>Contoso\svc_SCOM2012_dwwrite</b>	<b>Pa\$\$w0rd</b>

21. On the Help improve **Operations Manager** page, select **No, I am not willing to participate** in both sections, and then click **Next**.
22. On the **Microsoft Update** page, select **Off**, and then click **Next**.
23. On the **Installation Summary** page, click **Install**.
24. When the Installation is complete, cancel the selection for the **Start the Operations console when the wizard closes** option, and then click **Close**.

► **Task 2: Install the second Management Server**

1. Log on to LON-MS2.
2. Browse to **\LON-DC1\Media**, and then open the **SCOM2012R2** folder.
3. Double-click **Setup.exe** to start **Operations Manager** setup.
4. In the **Microsoft System Center 2012 R2** window that opens, click **Install**.
5. In the **Operations Manager Setup** wizard, on the **Select features to install** page, select **Management server** and **Operations console**, and then click **Next**.
6. On the **Select installation location** page, click **Next**.
7. On the **The Setup wizard cannot continue** page, notice that the **Report Viewer controls** are not installed.
8. Browse to **\LON-DC1\Media**, and then double-click **ReportViewer.msi**.
9. In the **Open File – Security Warning** window that opens, click **Run**.
10. On the opening page of the **Microsoft Report Viewer 2012 Runtime** wizard that starts, click **Next**.
11. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
12. On the **Ready to Install the Program** page click **Install**.
13. On the **Completing the Microsoft Report Viewer 2012 Runtime Installation** page, click **Finish**.
14. Go back to the **Operations Manager Setup** wizard, and then click **Verify Prerequisites Again**.
15. On the **Proceed with Setup** page, click **Next**.
16. On the **Specify an Installation option** page, select **Add a Management server to an existing management group**, and then click **Next**.

17. On the **Please read the license terms page**, select **I have read, understood and agree with the license terms**, and then click **Next**.
18. On the **Configure the operational database** page, in the **Server name and instance name** box, type **LON-SQ1**, press the Tab key on the keyboard, and then click the drop-down menu next to **Database name**. Click **OperationsManager**, and then click **Next**.
19. On the **Configure Operations Manager accounts** page, type the details as shown here and then click **Next**.

<b>Account Name</b>	<b>Domain\User Name</b>	<b>Password</b>
Management Server action account	<b>Contoso\svc_SCOM2012_msaa</b>	<b>Pa\$\$w0rd</b>
System Center Configuration service and System Center Data Access service	<b>Contoso\svc_SCOM2012_das</b>	<b>Pa\$\$w0rd</b>

20. On the **Help improve Operations Manager** page, select **No, I am not willing to participate** in both sections and then click **Next**.
  21. On the **Microsoft Update** page, select **Off** and then click **Next**.
  22. On the **Installation Summary** page, click **Install**.
  23. On the **Setup is complete** page, click **Close**.
- **Task 3: Install the Reporting server**
1. Log on to LON-SQ1.
  2. Click **Start**, then click **Internet Explorer** and then in the address bar type **http://LON-SQ1/Reports** and then press enter on the keyboard.
  3. Confirm the **SQL Server Reporting Services Home** page loads. This confirms SSRS is operating as expected.
  4. Close Internet Explorer.
  5. Browse to **\LON-DC1\Media**, and then open the **SCOM2012R2** folder.
  6. Double-click **Setup.exe** to start **Operations Manager** setup.
  7. If an **Open File – Security Warning** window opens, click **Run**.
  8. In the **Microsoft System Center 2012 R2** window that opens, click **Install**.
  9. In the **Operations Manager Setup** wizard, on the **Select features to install** page, select **Reporting server**, and then click **Next**.
  10. On the **Select installation location** page, click **Next**.
  11. On the **Proceed with Setup** page, click **Next**.
  12. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
  13. On the **Specify a Management Server** page, in the **Management server name** box, type **LON-MS1**, and then click **Next**.
  14. On the **SQL Server instance for reporting services** page, click **Next**.

15. On the **Configure Operations Manager accounts** page, type **Contoso\svc\_SCOM2012\_dwread** in the **Domain\User name** box, type **Pa\$\$w0rd** in the **Password** box, and then click **Next**.
  16. On the **Help improve Operations Manager** page, select **No, I am not willing to participate** in both sections, and then click **Next**.
  17. On the **Microsoft Update** page, select **Off**, and then click **Next**.
  18. On the **Installation Summary** page, click **Install**.
  19. On the **Setup is complete** page, click **Close**.
  20. Log on to **LON-MS1**, click **Start**, and then type **Operations**, then click **Operations Console**.
  21. Click the **Reporting** pane to confirm the Reporting Server is operational.
- **Task 4: Install the Web console server**
1. Log on to LON-MS1.
  2. Close the **Operations console** if it is open.
  3. Browse to **\LON-DC1\Media**, and then open the **SCOM2012R2** folder.
  4. Double-click **Setup** to start **Operations Manager** setup.
  5. In the **Microsoft System Center 2012 R2** window that opens, click **Install**.
  6. In the **Operations Manager Setup** wizard, on the **What do you want to do** page, select **Add a feature**.
  7. On the **Select features to install** page, select **Web Console**, and then click **Next**.
  8. On the Proceed with Setup page, click **Next**.
  9. On the **Specify a web site for use with the Web console** page, click **Next**.
  10. On the **Select an authentication mode for use with the Web console** page, click **Next**.
  11. On the Help improve Operations Manager page click Next.
  12. On the **Microsoft Update** page, select **Off**, and then click **Next**.
  13. On the **Installation Summary** page, click **Install**.
  14. On the **Setup is complete** page, click **Close**.
  15. Browse to **C:\Windows**, and then edit the security of the **Temp** folder.
  16. In the **Permissions for Temp** window that opens, edit **IIS\_IUSRS (LON-MS1\IIS\_IUSRS)** security, and then make sure that **Full Control** permissions are granted.
  17. Edit **NETWORK SERVICE**, and make sure that **Full Control** permissions are granted.
  18. Close the Permissions for Temp window.
  19. Click **Start**, and then click **Internet Explorer**.
  20. Browse to **http://LON-MS1/OperationsManager**.
  21. On the **Web Console Configuration Required** webpage, click **Configure**, and then when the **SilverlightClientConfiguration** window appears, click **Run**.
  22. In the **Web Console Configuration Tool** window, click **Close**.
  23. On the **Web Console Configuration Required** webpage, click **Skip**.
  24. Confirm the **Operations Manager Web Console** opens as expected.

---

25. Close Internet Explorer.

**Results:**

After this exercise, you should have performed a new installation of Microsoft System Center 2012 R2 Operations Manager. This includes two Management Servers: the Reporting Server and the Web console.

## Exercise 2: Installing and Configuring the Gateway Server

### ► Task 1: Import the root CA certificate chain on the Gateway Server

1. Log on to LON-GW1, and then open **Internet Explorer**.
2. Browse to <https://LON-AP2/certsrv>.
3. On the **There is a problem with this website's security certificate** webpage, click **Continue to the website (not recommended)**.
4. If a message that states **The Web Browser does not support the generation of certificate requests** appears, click the **Compatibility View** icon next to the **Certificate error** in the address bar.
5. On the **Microsoft Active Directory Certificate Services** webpage, click **Download a CA certificate, certificate chain or CRL**.
6. In the **Web Access Confirmation** window, click **Yes**.
7. On the **Download a CA Certificate, Certificate Chain, or CRL** webpage, click **Download CA certificate chain**.
8. In the **Do you want to open or save certnew.p7b (910 bytes) from LON-AP2?** window, click **Save** and then **Save As**.
9. In the **Save As** window that opens, click **This PC**, click **Desktop**, and then click **Save**.
10. **Close** the webpage.
11. Right-click **Start**, and then click **Run**.
12. In the **Open** box, type **MMC**, and then click **OK**.
13. In the **Console1 – [Console Root]** window that opens, on the **File** menu, click **Add/Remove Snap-in**.
14. In the **Add or Remove Snap-ins** window, under **Available snap-ins**, click **Certificates**, and then click **Add**.
15. On the **Certificates snap-in** window, select **Computer account**, and then click **Next**.
16. In the **Select Computer** window, click **Finish**.
17. In the **Add or Remove Snap-ins** window, click **OK**.
18. In the **Console1 – [Console Root]** window, expand **Console Root**, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
19. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
20. In the Certificate Import Wizard that opens, on the **Welcome to the Certificate Import Wizard** page, click **Next**.
21. On the **File to Import** page, click **Browse**.
22. In the **Open** window browse to the **Desktop**.
23. Click the drop-down menu, and then click **All Files (\*.\*)**.
24. Click **certnew**, and then click **Open**.
25. On the **File to Import** page, click **Next**.
26. On the **Certificate Store** page, click **Next**.
27. On the **Completing the Certificate Import Wizard** page, click **Finish**.
28. In the **Certificate Import Wizard** window, click **OK**.

29. Leave the **Console 1- [Console Root]** window open.

► **Task 2: Import the root CA certificate chain on the Management Server**

1. Log on to LON-MS2, and then open Internet Explorer.
2. Browse to <https://LON-AP2/certsrv>.
3. On the **There is a problem with this website's security certificate** webpage, click **Continue to the website (not recommended)**.
4. On the **Microsoft Active Directory Certificate Services** webpage, click **Download a CA certificate, certificate chain or CRL**.
5. In the Web Access Confirmation window, click Yes.
6. On the **Download a CA Certificate, Certificate Chain, or CRL** webpage, click **Download CA certificate chain**.
7. In the **Do you want to open or save certnew.p7b (910 bytes) from LON-AP2?** window, click the Save menu, and then click Save As.
8. In the **Save As** window that opens, browse to the **Desktop**, and then click **Save**.
9. Close the webpage.
10. Right-click **Start**, then click **Run**.
11. In the **Open** box, type **MMC** and then click **OK**.
12. In the **Console1 – [Console Root]** window that opens, on the **File** menu, click **Add/Remove Snap-in**.
13. In the **Add or Remove Snap-ins** window, under **Available snap-ins**, click **Certificates**, and then click Add.
14. In the **Certificates** snap-in window, select **Computer account**, and then click **Next**.
15. In the **Select Computer** window, click **Finish**.
16. In the **Add or Remove Snap-ins** window, click **OK**.
17. In the **Console1 – [Console Root]** window, expand **Console Root**, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
18. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
19. In the Certificate Import Wizard that starts, on the **Welcome to the Certificate Import Wizard** page, click **Next**.
20. On the **File to Import** page, click **Browse**.
21. In the **Open** window, browse to the **Desktop**.
22. Click the drop-down menu, and then click **All Files (\*.\*)**.
23. Click **certnew**, and then click **Open**.
24. On the **File to Import** page, click **Next**.
25. On the **Certificate Store** page, click **Next**.
26. On the **Completing the Certificate Import Wizard** page, click **Finish**.
27. In the Certificate Import Wizard window, click OK.
28. Leave the **Console 1- [Console Root]** window open.

► **Task 3: Request the Gateway Server certificate**

1. On LON-GW1, open Internet Explorer, and browse to <https://LON-AP2/certsrv>.
  2. On the **There is a problem with this website's security certificate** webpage, click **Continue to the website (not recommended)**.
  3. If a message stating **This Web browser does not support the generation of certificate requests** appears, click the **Compatibility View** button in the address bar.
  4. On the **Microsoft Active Directory Certificate Services** webpage, click **Request a certificate**.
  5. On the **Request a Certificate** webpage, click **Advanced certificate request**.
  6. On the **Advanced Certificate Request** webpage, click **Create and submit a request to this CA**.
  7. In the **Web Access Confirmation** window, click **Yes**.
  8. On the **Advanced Certificate Request** webpage, under **Type of Certificate Needed**, click the drop-down menu, and then click **Other**.
  9. In the **OID** box, type **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2**.
-  **Note:** Notice that a comma (,) is used in the middle of the OID value.
10. In the **Name** box, type **LON-GW1**.
  11. In the **Friendly Name** box, type **LON-GW1**.
  12. Select **Mark keys as exportable**.
  13. Click **Submit**, and then after the **Certificate Pending** page appears, click **Home**.
  14. Leave Internet Explorer open.

► **Task 4: Issue the Gateway Server certificate**

1. Log on to LON-AP2.
2. Click **Start**, click **Administrative Tools**, and then click **Certification Authority**.
3. In the **certsrv** window that opens, expand **Certification Authority (Local)**, then expand **LON-AP2**, and then click **Pending Requests**.
4. In the pane to the right, right-click the request, click **All Tasks**, and then click **Issue**.

► **Task 5: Import the Gateway Server certificate**

1. On LON-GW1, in Internet Explorer, on the **Microsoft Active Directory Certificate Services** webpage, click **View the status of a pending certificate request**.
2. Under **Select the certificate request you want to view**, click the request.
3. In the **Web Access Confirmation** window, click **Yes**.
4. On the **Certificate Issued** webpage, click **Install this certificate**.
5. When the **Certificate Installed** webpage appears, close Internet Explorer.
6. Right-click **Start**, and then click **Run**. In the **Open** box, type **MMC**, and then click **OK**.
7. In the **Console1 – [Console Root]** window that opens, on the **File** menu, click **Add/Remove Snap-in**.
8. In the **Add or Remove Snap-ins** window under **Available snap-ins**, click **Certificates**, and then click **Add**.
9. In the **Certificates snap-in** window, select **Computer account**, and then click **Next**.

10. In the **Select Computer** window, click **Finish**.
11. Click **Add** again, select **My user account** and then click **Finish**.
12. In the **Add or Remove Snap-ins** window, click **OK**.
13. In the **Console1 – [Console Root]** window, expand **Console Root**, expand **Certificates – Current User**, expand **Personal**, and then click **Certificates**.
14. In the pane to the right, right-click the certificate, click **All Tasks**, and then click **Export**.
15. In the **Certificate Export Wizard**, on the **Welcome to the Certificate Export Wizard** page, click **Next**.
16. On the **Export Private Key** page, select **Yes, export the private key**, and then click **Next**.
17. On the **Export File Format** page, click **Next**.
18. On the **Security** page, select **Password**; in the **Password** and **Confirm password** boxes and type **Pa\$\$w0rd** and then click **Next**.
19. On the **File to Export** page, click **Browse**; in the **Save As** window, click **Desktop**; in the **File name box**, type **LON-GW1**; and then click **Save**.
20. On the **File to Export** page, click **Next**, and then on the **Completing the Certificate Export Wizard** page, click **Finish**.
21. In the **Certificate Export Wizard** window, click **OK**.
22. In the **Console1 window**, expand **Certificate (Local Computer)**, and then click **Personal**.
23. Right-click **Personal**, click **All Tasks**, and then click **Import**.
24. In the Certificate Import Wizard, on the **Welcome to the Certificate Import Wizard** page, click **Next**.
25. On the **File to Import** page, click **Browse**.
26. In the **Open** window, click **Desktop**, and then next to the **Cancel** button, click the drop-down menu, and then click **All Files (\*.\*)**.
27. Click **LON-GW1**, and then click **Open**.
28. On the **File to Import** page, click **Next**.
29. On the **Private key protection** page, in the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
30. On the **Certificate Store** page, click **Next**.
31. On the **Completing the Certificate Import Wizard** page, click **Finish**.
32. In the **Certificate Import Wizard** window, click **OK**.

► **Task 6: Request the Management Server certificate**

1. On LON-MS2, open Internet Explorer, and the browse to <https://LON-AP2/certsrv>.
2. On the **There is a problem with this website's security certificate** webpage, click **Continue to the website (not recommended)**.
3. On the **Microsoft Active Directory Certificate Services** webpage, click **Request a certificate**.
4. On the **Request a Certificate** webpage, click **Advanced certificate request**.
5. On the Advanced Certificate Request webpage, click Create and submit a request to this CA.
6. In the Web Access Confirmation window, click Yes.

7. On the Advanced Certificate Request webpage, click the Type of Certificate Needed menu, and then click Other.
8. In the OID box, type **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2**
-  **Note:** Notice that a comma (,) is used in the middle of the OID value.
9. In the Name box type LON-MS2.contoso.com.
10. In the Friendly Name box, type LON-MS2.contoso.com.
11. Select Mark keys as exportable.
12. Click **Submit**, and then after the **Certificate Pending** page appears, click **Home**.
13. Leave Internet Explorer open.

► **Task 7: Issue the Management Server certificate**

1. Log on to LON-AP2.
2. Click **Start, Administrative Tools**, and then click **Certification Authority**.
3. In the **certsrv** window that opens, expand **Certification Authority (Local)**, expand **LON-AP2**, and then click **Pending Requests**.
4. In the pane to the right, right-click the request, click **All Tasks**, and then click **Issue**.

► **Task 8: Import the Management Server certificate**

1. On LON-MS2, in Internet Explorer, on the **Microsoft Active Directory Certificate Services** webpage, click **View the status of a pending certificate request**.
2. Under **Select the certificate request you want to view**, click the request.
3. In the **Web Access Confirmation** window, click **Yes**.
4. On the **Certificate Issued** webpage, click **Install this certificate**.
5. When the **Certificate Installed** webpage appears, close Internet Explorer.
6. Right-click **Start**, click **Run**; in the **Open** box, enter **MMC**; and then click **OK**.
7. In the **Console1 – [Console Root]** window that opens, on the **File** menu, click **Add/Remove Snap-in**.
8. In the **Add or Remove Snap-ins** window, under **Available snap-ins**, click **Certificates**, and then click **Add**.
9. In the **Certificates snap-in** window, select **Computer account**, and then click **Next**.
10. In the **Select Computer** window, click **Finish**.
11. Click **Add** again, select **My user account** and then click **Finish**.
12. In the **Add or Remove Snap-ins** window, click **OK**.
13. In the **Console1 – [Console Root]** window, expand **Console Root**, expand **Certificates – Current User**, expand **Personal**, and then click **Certificates**.
14. In the pane to the right, right-click the certificate, click **All Tasks**, and then click **Export**.
15. In the **Certificate Export Wizard**, on the **Welcome to the Certificate Export Wizard** page, click **Next**.
16. On the **Export Private Key** page, select **Yes, export the private key**, and then click **Next**.
17. On the **Export File Format** page, click **Next**.

18. On the **Security** page, select **Password** and then in the **Password** and **Confirm password** boxes type **Pa\$\$w0rd**; and then click **Next**.
19. On the **File to Export** page, click **Browse**; in the **Save As** window, click **Desktop**; in the **File name box**, type **LON-MS2**; and then click **Save**.
20. On the **File to Export** page, click **Next**, and on the **Completing the Certificate Export Wizard** page, click **Finish**.
21. In the **Certificate Export Wizard** window, click **OK**.
22. In the **Console1 window**, expand **Certificate (Local Computer)**, and then click **Personal**.
23. Right-click **Personal**, click **All Tasks**, and then click **Import**.
24. In the Certificate Import Wizard, on the **Welcome to the Certificate Import Wizard** page, click **Next**.
25. On the **File to Import** page, click **Browse**.
26. In the **Open** window, click **Desktop**, and then click the drop-down menu, and then click **All Files (\*.\*)**.
27. Click **LON-MS2**, and then click **Open**.
28. On the **File to Import** page, click **Next**.
29. On the **Private key protection** page, in the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
30. On the **Certificate Store** page, click **Next**.
31. On the **Completing the Certificate Import Wizard** page, click **Finish**.
32. In the **Certificate Import Wizard** window, click **OK**.

► **Task 9: Import the Management Server certificate into Operations Manager and approve the Gateway Server**

1. On LON-MS2, browse to **\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64**.
2. Double-click **MOMCertImport.exe**, and in the **Windows Security** window, click **LON-MS2.contoso.com**, and then click **OK**.
3. From **\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64** copy **Microsoft.EnterpriseManagement.GatewayApprovalTool.exe** to **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server**.
4. Open a command prompt window, and then browse to **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server**.
5. Type the following, and then press Enter.

```
Microsoft.EnterpriseManagement.GatewayApprovalTool.exe /ManagementServerName=LON-MS2.CONTOSO.COM /GatewayName=LON-GW1 /SiteName=London /Action/Create
```

6. When a message that states **The approval of server LON-GW1 completed successfully** is displayed, close the command prompt window.

► **Task 10: Install the Gateway Server**

1. On LON-GW1, browse to **C:\Gateway\AMD64**.
2. Double-click **MOMGateway**.
3. In the **System Center 2012 R2 Operations Manager Gateway** window, click **OK**.

4. In the **System Center 2012 R2 Operations Manager Gateway Server Setup** wizard, on the **Welcome to the System Center 2012 R2 Operations Manager Gateway Server Setup wizard** page, click **Next**.
5. On the **IMPORTANT NOTICE** page, click **I Agree**.
6. On the **Destination Folder** page, click **Next**.
7. On the **Management Group Configuration** page, in the **Management Group Name** box, type **SCOM2012**.
8. In the **Management Server** box, Type **LON-MS2.contoso.com**, and then click **Next**.
9. On the **Gateway Action Account** page, select **Local System**, and then click **Next**.
10. On the **Microsoft Update** page, click **Next**.
11. On the **Ready to Install** page, click **Install**.
12. On the **Completing the System Center 2012 R2 Operations Manager Gateway Server Setup wizard** page, click **Finish**.

► **Task 11: Import the Gateway Server certificate into Operations Manager**

1. On LON-GW1, browse to **\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64**.
2. Double-click **MOMCertImport.exe**, and if the **Open File – Security Warning** window opens, click **Run**.
3. Click LON-GW1, and then click **OK**.

► **Task 12: Confirm the Gateway Server is communicating with the Management Server**

1. On LON-MS2, open the Operations console.
2. Click the **Administration** pane, expand **Device Management**, and then click **Management Servers**.
3. Right-click the **Details** pane, and then click **Refresh**.
4. Confirm that the Gateway Server **LON-GW1** is displayed with a health state of **Healthy**.



**Note:** It can take up to 5 minutes for the **LON-GW1** server to appear.

**Results:** After this exercise, you should have installed and configured an Operations Manager Gateway Server on LON-GW1. This involves importing the root certificate chain on both the Gateway Server, and the Management Server that will manage the Gateway Server. Then, you would have requested, issued, and imported a server certificate for both the Management Server and the Gateway Server. Finally, you will have installed the Gateway Server on LON-GW1, and then used the MOMCertImport tool to import the Gateway Server certificate into Operations Manager.

## Exercise 3: Installing the Operations Manager Agent

### ► Task 1: Perform a push-install of the Operations Manager agent

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, and then click the **Discovery Wizard** link that is located just above the **Monitoring** pane.
3. In the Computer and Device Management wizard, on the **Discovery Type** page, make sure **Windows computers** is selected, and then click **Next**.
4. On the **Auto or Advanced** page, make sure **Advanced discovery** is selected.
5. Click the Management Server menu, click **LON-MS1.CONTOSO.COM**, and then click **Next**.
6. On the **Discovery Method** page, select **Browse for, or type-in computer names**. Then in the text box underneath this, type **LON-SQ1, LON-DC1** and then click **Next**.
7. On the **Administrator Account** page, select **Other user account**.
8. In the **User name** text box, type **Administrator**, then in the **Password** box type **Pa\$\$w0rd**; and then click **Discover**.
9. On the **Select Objects to Manage** page, select **LON-SQ1.contoso.com** and **LON-DC1.contoso.com** and then click **Next**.
10. On the **Summary** page, click **Finish**.
11. In the **Agent Management Task Status** window that opens, monitor the **Task Output** column until a message that states the task completed successfully appears, and then click **Close**.
12. Confirm that the **LON-SQ1.contoso.com** and **LON-DC1.contoso.com** computers are now displayed in the **Agent Managed** view of the **Device Management** folder in the **Administration** node of the **Administration** pane.



**Note:** The computers first display a Health State of not monitored. This changes to Healthy after approximately two minutes.

### ► Task 2: Allow manual agent installations in Operations Manager

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, and then click **Settings**.
3. In the **Details** pane, double-click **Security**.
4. In the **Global Management Server Settings – Security** window that opens, on the **General** tab, select **Review new manual agent installations in pending management view**, and then click **OK**.

### ► Task 3: Install the Operations Manager agent manually

1. Log on to LON-AP2, and then browse to the **\\\LON-DC1\Media\SCOM2012R2\Agent\AMD64** folder, and double-click **MOMAgent.msi**.
2. If an **Open File – Security Warning** window appears, click **Run**.
3. In the Microsoft Monitoring Agent Setup wizard, on the **Welcome to the Microsoft Monitoring Agent Setup Wizard** page, click **Next**.
4. On the **Important Notice** page, click **I Agree**.
5. On the **Destination Folder** page, click **Next**.

6. On the **Agent Setup Options** page, click **Next**.
7. On the **Management Group Configuration** page, in the **Management Group Name** box, type **SCOM2012**. In the **Management Server** box, type **LON-MS1**, and then click **Next**.
8. On the **Agent Action Account** page, click **Next**.
9. On the **Ready to Install** page, click **Install**.
10. On the **Microsoft Monitoring Agent configuration completed successfully** page, click **Finish**.

► **Task 4: Use the Operations console to approve a manually installed agent**

1. Log on to LON-MS1, and open the Operations console.
2. Click the **Administration** pane, and then expand the **Administration** node.
3. Expand Device Management, and then click Pending Management.
4. In the **Details** pane, click **LON-AP2.contoso.com**, and then in the **Tasks** pane, click **Approve**.
5. In the **Manual Agent Install** dialog box, click **Approve**.
6. Under **Device Management**, click **Agent Managed**, and then confirm that **LON-AP2** is displayed.

**Results:** After this exercise, you should have installed an Operations Manager agent using the Operations console. You should have also configured Operations Manager to review new manual agent installations and then manually installed and approved an Operations Manager Agent.

## Exercise 4: Configuring Active Directory Integration

- **Task 1: Use Momadadmin.exe to configure the Active Directory container**
1. On LON-MS1, open a Command Prompt window, and then browse to **C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server**.
  2. Type the following command, and then press Enter.

```
MomAdAdmin.exe SCOM2012 Contoso\SCOM2012_Admins Contoso\Administrator Contoso
```
  3. Close the Command Prompt window.
- **Task 2: Configure the Active Directory Based Agent Assignment Account Run As Profile**
1. Log on to LON-MS1, and open the Operations console.
  2. Click the **Administration** pane, expand **Run As Configuration**, and then click **Profiles**.
  3. In the details pane, right-click **Active Directory Based Agent Assignment Account**, and then click **Properties**.
  4. In the Run As Profile Wizard that starts, on the **Introduction** page, click **Next**.
  5. On the **General Properties** page, click **Next**.
  6. On the **Run As Accounts** page click **Add**.
  7. In the **Add a Run As Account** window that opens, click **New**.
  8. In the Create Run As Account Wizard that starts, on the **Introduction** page, click **Next**.
  9. On the **General Properties** page, in the **Display name** box, enter **Administrator**, and then click **Next**.
  10. On the **Credentials** page, in the **User name** box, enter **Administrator**.
  11. In the **Password** and **Confirm password** boxes, Enter **Pa\$\$w0rd**, and then click **Next**.
  12. On the **Distribution Security** page, click **Create**.
  13. On the **Completion** page, click **Close**.
  14. In the **Add a Run As Account**, select **A selected class, group or object**, and then click **Select**.
  15. Click **Group**, and in the **Group Search** window that opens, in the **Filter by (optional)** box, type **AD**, and then click **Search**.
  16. Under **Available Groups**, click **AD Assignment Resource Pool**, and then click **OK**.
  17. In the **Add a Run As Account** window, click **OK**.
  18. On the **Run As Accounts** page, click **Save**.
  19. On the **Completion** page, click the **Administrator** link.
  20. In the **Run As Account Properties – Administrator** window that opens, click **Add**.
  21. In the **Computer Search** window that opens, in the **Filter by (optional)** box, type **MS**, and then click **Search**.
  22. Under **Available items**, select both **LON-MS1.CONTOSO.COM** and **LON-MS2.CONTOSO.COM**, click **Add**, and then click **OK**.
  23. In the **Run As Account Properties – Administrator** window, click **OK**.

24. In the **Run As Profile Wizard**, click **Close**.
25. Under the **Security** node in the **Administration** pane, click **User Roles**.
26. In the details pane, right-click **Operations Manager Administrators**, and then click **Properties**.
27. In the **Operations Manager Administrators – User Role Properties** window that opens, on the **General Properties** page, click **Add**.
28. In the **Select Group** window that opens, in the **Enter the object name to select** box, type **SCOM2012\_Admins**, and then click **Check Names**.
29. In the **Select Group** window, click **OK**, and then in the **Operations Manager Administrators – User Role Properties** window, click **OK**.

► **Task 3: Use the Agent Assignment and Failover Wizard**

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, expand **Device Management**, and then click **Management Servers**.
3. Right-click **LON-MS1**, and then click **Properties**.
4. In the **LON-MS1.CONTOSO.COM – Management Server Properties** window that opens, on the **Auto Agent Assignment** tab, click **Add**.
5. In the Agent Assignment and Failover Wizard that starts, on the **Introduction** page, click **Next**.
6. On the **Domain** page, click **Next**.
7. On the **Inclusion Criteria** page, click **Configure**.
8. In the **Find Computers** window that opens, in the **Computer name** box, type **LON-AP1**, and then click **OK**.
9. On the **Inclusion Criteria** page, click **Next**.
10. On the **Exclusion Criteria** page, click **Next**.
11. On the **Agent Failover** page, click **Create**.
12. On the **LON-MS1.CONTOSO.COM – Management Server Properties** page, click **OK**.

► **Task 4: Install the agent using Momagent.msi**

1. Log on to LON-AP1, browse to **\LON-DC1\Media\SCOM2012R2\agent\AMD64**, and then double-click **MOMAgent.msi**.
2. In the **Microsoft Monitoring Agent Setup** wizard that starts, on the **Welcome to the Microsoft Monitoring Agent Setup Wizard** page, click **Next**.
3. On the **Important Notice** page, click **I agree**.
4. On the **Destination Folder** page, click **Next**.
5. On the **Agent Setup Options** page, cancel the **Connect the agent to System Center Operations Manager** selection, and then click **Next**.
6. On the **Microsoft Update** page, click **Next**.
7. On the **Ready to Install** page, click **Install**.
8. On the **Microsoft Monitoring Agent configuration completed successfully** page, click **Finish**.

► **Task 5: Confirm the agent is automatically assigned**

1. Log on to LON-MS1, and open the Operations console.

2. Click the Administration pane, expand **Device Management**, and then click **Pending Management**.
3. In the details pane, click **LON-AP1**, and then in the **Tasks** pane, click **Approve**.
4. In the **Manual Agent Install** window that opens, click **Approve**.
5. Click the **Agent Managed** view, and then confirm **LON-AP1** is displayed.

 **Note:** It can take up to 15 minutes for the agent to appear in the **Pending Management** view.

 **Note:** If after 15 minutes the agent does not appear in the **Pending Management** view on LON-AP1 restart the **Microsoft Monitoring Agent** service and the refresh the **Pending Management** view. If the agent still does not appear perform the following steps on LON-MS1:

1. In the **Operations console** on LON-MS1 click the **Authoring** pane and then expand **Management Pack Objects** and then click **Rules**.
2. From the center pane click **Change Scope**.
3. In the **Scope Management Pack Objects** window that opens click **Clear All** (if it is available) and then click **View all targets**.
4. In the **Look for** box type **AD**.
5. Select the check box for both **AD Assignment Resource Pool** targets and then click **OK**.
6. From the center pane right-click **AD rule for Domain: CONTOSO.COM, ManagementServer: CONTOSO\LON-MS1** and then click **Overrides**, then click **Override this Rule**, then click **For all objects of class: AD Assignment Resource Pool**.
7. In the **Override Properties** window that opens select the **Override** check box for the **Frequency** parameter.
8. In the **Override Value** box for the **Frequency** parameter remove **3600** and then type **300**.
9. Click **OK** on the **Override** window.
10. Wait for **6** minutes and then on LON-AP1 open Windows Services and then restart the **Microsoft Monitoring Agent** service.

**Results:** After completing this exercise you should have configured Active Directory Integration in Operations Manager. You should have also confirmed that integration is working as expected by manually installing an agent and then confirming that it is automatically assigned to the relevant Management Server.

## Exercise 5: Installing and Configuring Audit Collection Services (ACS)

### ► Task 1: Configure the security event log

11. Log on to LON-DC1, click **Start**, and then click **Administrative Tools**.
12. In the **Administrative Tools** window that opens, double-click **Local Security Policy**.
13. In the **Local Security Policy** window that opens, expand **Local Policies**, and then click **Audit Policy**.
14. In the Details pane, double-click Audit account Logon events.
15. In the **Audit account Logon events Properties** window that opens, select **Success** and **Failure**, and then click **OK**.
16. Double-click Audit Logon events, and in the Audit Logon events Properties window that opens, select Success and Failure.
17. Click **OK**.
18. Close the **Local Security Policy** window, and then log off from **LON-DC1**.

### ► Task 2: Install the ACS Collector

1. Log on to LON-MS2, browse to **\LON-DC1\Media\SCOM2012R2**, and then double-click **Setup**.
2. In the **Microsoft System Center 2012 R2** window that opens, under **Optional Installations**, click **Audit collection services**.
3. In the Audit Collection Services Collector Setup wizard that opens, on the **Welcome to the Audit Collection Services Collector Setup Wizard** page, click **Next**.
4. On the **Microsoft Software License Terms** page, select **I accept the license terms**, and then click **Next**.
5. On the **Database Installation Options** page, click **Next**.
6. On the **Data Source** page, click **Next**.
7. On the **Database** page, in the **Remote database server machine name** text box, type **LON-SQ1** and then click **Next**.
8. On the **Database Authentication** page, click **Next**.
9. On the **Database Creation Options** page, select **Use SQL Server's default data and log file directories**, and then click **Next**.
10. On the **Event Retention Schedule** page, click **Next**.
11. On the **ACS Stored Timestamp Format** page, click **Next**.
12. On the **Summary** page, click **Next**.
13. In the **SQL Server Login** window that opens, click **OK**.
14. On the **Audit Collection Services installation failed** page, click **Finish**.
15. Confirm that the ADTServer service has started by opening a Command Prompt window and typing:

```
Net start ADTServer
```

16. "The requested service has already been started" message is displayed, and confirms that the service is running.

### ► Task 3: Configure the ACS Forwarder

1. Log on to LON-MS1, and then open the Operations console.

2. Click the **Monitoring** pane, and then expand **Operations Manager**.
3. Expand **Agent Details**, and then click **Agents By Version**.
4. In the details pane, click **LON-DC1.CONTOSO.COM**.
5. In the **Tasks** pane, under **Health Service Tasks**, click **Enable Audit Collection**.
6. In the **Run Task – Enable Audit Collection** window that opens, click **Override**.
7. In the **Override Task Parameters** window that opens, in the **New Value** box, type **LON-MS2.CONTOSO.COM**, and then click **Override**.
8. In the **Run Task – Enable Audit Collection** window, click **Run**.
9. In the **Tasks Status – Enable Audit Collection** window that opens, wait for the task to complete successfully, and then click **Close**.

#### ► Task 4: Configure ACS filtering

1. Log on to LON-MS2, and then open a Command Prompt window as an Administrator.
2. Open Registry Editor by using **regedit32**.
3. Browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer**.
4. Right-click **Parameters**, and then click **Permissions**.
5. In the **Permissions for Parameters** window that opens, under **Group or user names**, click **NETWORK SERVICE**.
6. Select the **Allow** for the **Full Control** permission, and then click **OK**.
7. Close Registry Editor.
8. At the command prompt, browse to **C:\Windows\System32\Security\ADTServer**.
9. Type the following command, and then press Enter.

```
AdtAdmin /getquery
```



**Note:** The returned value shows that currently ACS is collecting all events.

10. Type the following command, and then press Enter.

```
AdtAdmin /setquery /query:"SELECT * FROM AdtsEvent WHERE NOT (HeaderUser='SYSTEM')"
```

11. Type the following command, and then press Enter.

```
AdtAdmin /getquery
```



**Note:** The ACS now filters out any events that the System generates.

#### ► Task 5: Configure ACS reporting

1. Log on to LON-MS2, browse to **\LON-DC1\Media\SCOM2012R2\ReportModels**, and then copy the **ACS** folder.
2. Paste the **ACS** folder to drive **C** on LON-MS2.
3. Open a Command Prompt window, and then browse to the **C:\ACS** folder.

4. Type the following command, and then press Enter.

```
UploadAuditReports LON-SQ1 http://LON-SQ1/ReportServer C:\acs
```

5. Wait for the Command Prompt window to return to the **C:\acs>** command prompt.
6. Open the Operations console, and then click the **Reporting** pane.
7. Expand **Reporting**, and then click **Audit Reports**.

 **Note:** The ACS reports are now displayed in the **Details** pane.

### ► Task 6: View ACS reports

1. On LON-DC1, if **Administrator** is logged on to the computer, log the **Administrator** off the computer.
2. Try to log on to **LON-DC1** three times by using the **Contoso\Administrator** account and an incorrect password.
3. Change the user, and try to log on another three times by using a user name of **FailedLogon** and any password.
4. On LON-MS2, open the Operations console, and then click the **Reporting** pane.
5. Expand **Reporting**, and then click **Audit Reports**.
6. In the **Details** pane, click the **Access\_Violation\_-\_Unsuccessful\_Logon\_Attempts** report.
7. In the **Tasks** pane, click **Open**.
8. In the **Unsuccessful Logon Attempts** report that opens, view the failed logon attempts that were recorded for the **FailedLogon** user account.
9. Close the **Report** window.

**Results:** After this exercise, you should have installed and configured ACS in System Center 2012 R2 Operations Manager. You should have also configured security event logging on the domain controller LON-DC1 and simulated several failed logon attempts. Finally, you should have viewed the Access\_Violation\_-\_Unsuccessful\_Log on\_Attempts report to view the failed logon attempts.

## Exercise 6: Configuring Agentless Exception Monitoring (AEM)

### ► Task 1: Configure a Management Server for client monitoring

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, and then under **Device Management**, click **Management Servers**.
3. From the **Details** pane, right-click **LON-MS1**, and then click **Configure Client Monitoring**.
4. In the Client Monitoring Configuration Wizard, on the **Introduction** page, click **Next**.
5. On the **CEIP Forwarding** page, select **Yes, use the selected Management Server to collect and forward CEIP data to Microsoft**.
6. Clear **Use Secure Sockets Layer (SSL) protocol**, and then click **Next**.
7. On the **Error Collection** page, in the **File Share Path** box, type **C:\AEM**.
8. Clear **Use Secure Sockets Layer (SSL) protocol**, and then click **Next**.
9. On the **Error Forwarding** page, select **Forward all collected errors to Microsoft (Recommended)**, and then click **Next**.
10. On the **Create File Share** page, select **Other user account (will not be saved)**, and in the **User name** box, type **Administrator**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
12. On the **Task Status** page, click **Next**.
13. On the **Client Settings** page, click **Browse**.
14. In the **Browse For Folder** window that opens, click **Desktop**, and then click **OK**.
15. On the **Client Settings** page, click **Finish**.

### ► Task 2: Configure clients for client monitoring

1. Logon to LON-MS1, and then copy the **LON-MS1.CONTOSO.COM.ADM** file from the desktop to **\\\LON-DC1\C\$**.
2. Log on to LON-DC1, click **Start**, and then click **Administrative Tools**.
3. In the **Administrative Tools** window that opens, double-click **Group Policy Management**.
4. Expand **Forest:Contoso.com**, expand **Domains**, and then expand **contoso.com**.
5. Right-click **Default Domain Policy**, and then click **Edit**.
6. In the **Group Policy Management Editor** window that opens, expand the following:
  - a. **Computer Configuration**
  - b. **Policies**
  - c. **Administrative Templates**
  - d. **System**
  - e. **Internet Communication Management**
7. Click **Internet Communication Settings**.
8. From the **Details** pane, double-click **Turn off Windows Error Reporting**.
9. In the **Turn off Windows Error Reporting** window that opens, select **Disabled**, and then click **OK**.

10. Under **Computer Configuration**, expand **Policies**, right-click **Administrative Templates**, and then click **Add/Remove Templates**.
11. In the **Add/Remove Templates** window that opens, click **Add**.
12. Browse to drive **C**, click the **LON-MS1.CONTOSO.COM.adm** file, and then click **Open**.
13. In the **Add/Remove Templates** window, click **Close**.
14. Under **Administrative Templates**, expand the following:
  - a. **Classic Administrative Templates (ADM)**
  - b. **Microsoft Applications**
  - c. **System Center Operations Manager (SCOM)**
15. Click **SCOM Client Monitoring CEIP Settings**.
16. In the **Details** pane, double-click **Configure CEIP (Customer Experience Improvement Program)**.
17. In the **Configure CEIP (Customer Experience Improvement Program)** window that opens, select **Enabled**, and then click **OK**.
18. Under **System Center Operations Manager (SCOM)**, click **SCOM Client Monitoring**.
19. In the **Details** pane, double-click **Configure Error Reporting for Windows Vista and later operating systems**.
20. In the **Configure Error Reporting for Windows Vista and later operating systems** window that opens, select **Enabled**, and then click **OK**.
21. In the **Details** pane, double-click **Configure Error Notification**.
22. In the **Configure Error Notification** window that opens, select **Enabled**, and then click **OK**.
23. In the **Details** pane, double-click **Configure Error Reporting for Windows Operating Systems older than Windows Vista**.
24. In the **Configure Error Reporting for Windows Operating Systems older than Windows Vista** window that opens, select **Enabled**, and then click **OK**.
25. Expand **SCOM Client Monitoring**, and then click **Advanced Error Reporting settings**.
26. In the **Details** pane, double-click **Application reporting settings (all or none)**.
27. In the **Application reporting settings (all or none)** window that opens, select **Enabled**, and then click **OK**.
28. In the **Details** pane, double-click **Report operating system errors**.
29. In the **Report operating system errors** window that opens, select **Enabled**, and then click **OK**.
30. In the **Details** pane, double-click **Report unplanned shutdown events**.
31. In the **Report unplanned shutdown events** window that opens, select **Enabled**, and then click **OK**.
32. Close the **Group Policy Management Editor** window.
33. Close the **Group Policy Management** window.

► **Task 3: Simulate an exception and view AEM data**

1. Log on to LON-MS2, and then open a Command Prompt window.
2. Browse to the **C:\AEMValidation** folder.
3. Type the following command, and then press Enter.

```
gpupdate /force
```

4. Type the following command, and then press Enter.

```
AEMTestApplication 0
```

5. In the **AEMTestApplication.exe** window that opens, click **Check online for a solution and close the program**.
6. Click **Send Information**.
7. Open the Operations console, and then click the **Monitoring** pane.
8. Expand **Agentless Exception Monitoring**, and then click **Error Group View**.
9. From the **Details** pane, view the **AEMTESTAPPLICATION.EXE** application that is listed.
10. Click the **Error Events** view, and then note the error events that were generated.
11. Click **Crash Listener View**, and in the **Details** pane, click **LON-MS1.CONTOSO.COM**.
12. In the **Tasks** pane, under **Report Tasks**, click **Availability**.
13. In the **Availability – Operations Manager – Report – SCOM2012** window that opens, change the **From** field to **Yesterday**, and then click **Run**.
14. In the **Availability Report**, click **Availability Tracker** to view the availability of the AEM Crash Listener.

**Results:** After this exercise, you should have configured Agentless Exception Monitoring in System Center 2012 R2 Operations Manager. You should also have used the AEMTestApplication utility to simulate an application crash on LON-MS2, and then used views and reports in Operations Manager to view the crash details.



# Module 3: Upgrading Operations Manager

## Lab: Upgrading to System Center 2012 R2 Operations Manager

### Exercise 1: Preparing the Operations Manager 2007 R2 Environment for Upgrade

#### ► Task 1: Confirm the Operations Manager version

1. Log on to **LON-RMS**.
2. From the desktop, double-click **Operations Console** to start the SCOM 2007 R2 console.
3. Click the **Monitoring** pane, and then click the **Agents by Version** view.

 **Note:** Notice that the **Patch List** column shows that the agent running on the domain controller **LON-DC1** is at **CU5**.

4. Open Windows Explorer, and then browse to the **C:\Program Files\System Center Operations Manager 2007** folder.
5. Right-click the **HealthService.dll** file, and then click **Properties**.
6. In the properties window, click the **Details** tab, and notice the **File Version** displays **6.1.7221.81**. This indicates CU5.
7. In the **HealthService.dll** properties window, click **OK**.

#### ► Task 2: Import the Upgrade Helper management pack

1. Log on to LON-RMS, browse to the **Media** share on \\LON-DC1, and then browse to the **SCOM2012\MANAGEMENTPACKS** folder.
2. Copy the **OPERATIONSMANAGER.UPGRADE.MP** file and paste it on the **LON-RMS** desktop.
3. Open the Operations console, click the **Administration** pane, and then click **Management Packs**.
4. In the **Actions** pane, click **Import Management Packs**.
5. In the **Select Management Packs** window, click **Add**, and then click **Add from Disk**.
6. In the **Online Catalog Connection** pop-up window, click **No**.
7. Browse to the desktop, select the **OperationsManager.Upgrade.mp** file, and then click **Open**.
8. Click **Install** to install the Management Pack.
9. After several seconds, the **Import Management Packs** window will show the Management Pack is successfully installed.
10. Click **Close** to close the **Import Management Packs** window.
11. Click the **Monitoring** pane, and notice the new **Operations Manager Upgrade MP** views.

#### ► Task 3: Move agents that report to the RMS to a secondary Management Server

1. Log on to LON-RMS, and then open the Operations console.
2. Click the Administration pane, expand Device Management, and then click Agent Managed.



**Note:** Notice that the primary Management Server for **LON-DC1** is currently the Root Management Server (RMS) **LON-RMS**.

3. Right-click **LON-DC1**, and then click **Change Primary Management Server**.
4. In the **Change Management Server** window that opens, click **LON-MG1**, and then click **OK**.
5. Notice that the primary Management Server for **LON-DC1** is now **LON-MG1**.

#### ► Task 4: Back up the encryption key

1. Log on to LON-RMS, and then open a Command Prompt window by using the **Run as Administrator** option.
2. In the **Administrator: Command Prompt** window that opens, change the directory to the **C:\Program Files\System Center Operations Manager 2007** folder, and then type the following.

```
SecureStorageBackup Backup c:\encryptionkey.snk
```

3. Press Enter to execute the command.
4. When you are prompted for a password, type **Pa\$\$w0rd**, and then press Enter.
5. Type **Y**, and then press **Enter**.
6. Enter the password again when you are prompted.
7. When the message **Key successfully backed up to c:\encryptionkey** appears, close the **Administrator: Command Prompt** window.
8. Open **Windows Explorer**, and then browse to **Local Disk (C:)**.
9. Confirm that the **encryptionkey** file is present.

#### ► Task 5: Review the Operations Manager 2007 R2 event logs

1. Log on to LON-RMS, click **Start**, click **Administrative Tools**, and then click **Event Viewer**.
2. In the **Event Viewer** window that opens, expand **Applications and Services Logs**, and then click **Operations Manager** to view the Operations Manager event logs.
3. Review any warning, error or critical events.
4. Repeat steps 1 through 3 and replace LON-RMS with **LON-MG1**.

#### ► Task 6: Remove agents from pending management

1. Log on to LON-RMS, and then open the Operations console.
2. Click the **Administration** pane, and then expand **Device Management**.
3. Click **Pending Management**, and then in the **Details** pane, confirm that there are no computers in a pending management state.
4. If **LON-DC1** is listed, select it; in the **Actions** pane, click **Approve**; then in the **Agent Management Task Status** window that opens, click **Run Task**.

#### ► Task 7: Verify SQL Server and database collation

1. Log on to LON-RMS, click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** window, click **Connect**.
3. In Microsoft SQL Server Management Studio, click **New Query**.

4. In the **SQLQuery1.sql** window, type the following.

```
SELECT DATABASEPROPERTYEX ('OperationsManager','collation') SQLcollation
```

5. Click **Execute**.

 **Note:** Notice that in the **Results** pane, **SQLcollation** is listed as **SQL\_Latin1\_General\_CI\_AS**.

► **Task 8: Verify that the operational database has enough free space**

1. Log on to LON-RMS, click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** window, click **Connect**.
3. In Microsoft SQL Server Management Studio, expand **Databases**, right-click the **OperationsManager** database, and then click **Properties**.
4. In the **Database Properties – OperationsManager** window that opens, on the **General** tab, in the right pane, under **Database**, view the **Size and Space Available** fields to determine whether there is more than 50 percent of free space available.
5. Click the **Files** tab, and then under **Database files**, in the **Initial Size (MB)** column for **MOM\_DATA**, type **1500** to replace the value that is listed.
6. In the **Database Properties – OperationsManager** window, click **OK**.

► **Task 9: Backup the Operations Manager databases**

1. Log on to LON-RMS, click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** window, click **Connect**.
3. In Microsoft SQL Server Management Studio, expand **Databases**, right-click the **OperationsManager** database, click **Tasks**, and then click **Back Up**.
4. In the **Back Up Database – Operations Manager** window, click **OK** to back up the **OperationsManager** database.
5. In the Microsoft SQL Server Management Studio pop-up window, click **OK**.
6. Right-click the **OperationsManagerDW** database, click **Tasks**, and then click **Back Up**.
7. In the **Back Up Database – Operations ManagerDW** window, click **OK** to back up the **OperationsManagerDW** database.
8. In the **Microsoft SQL Server Management Studio** pop-up window, click **OK**.
9. Close the Microsoft SQL Server Management Studio window.
10. If prompted, click **No** on the Microsoft SQL Server Management Studio window.

► **Task 10: Restore the encryption key on the secondary Management Server**

1. Copy, from drive C on LON-RMS to drive C on LON-MG1, the **C:\encryptionkey.snk** file that is created in the "Back up the encryption key" task.
2. Log on to LON-MG1, and then open a Command Prompt window by using the **Run as Administrator** option.
3. In the **Administrator: Command Prompt** window that opens, change the directory to the **C:\Program Files\System Center Operations Manager 2007** folder, and then type the following.

```
SecureStorageBackup Restore c:\encryptionkey.snk
```

4. Press Enter to execute the command.
5. When you are prompted for the password, type **Pa\$\$w0rd**, and then press Enter.
6. When the message Key successfully restored from c:\ encryptionkey appears, close the Administrator: Command Prompt window.

**Results:** After this exercise, you should have performed the necessary preupgrade tasks for Center Operations Manager 2007 R2 upgrade in this environment. You should know the preupgrade tasks and the order in which they are performed for this specific environment. The tasks and order in other environments could be different based on how Operations Manager 2007 R2 is deployed.

## Exercise 2: Upgrading the Operations Manager 2007 R2 Management Group to System Center 2012 Operations Manager

### ► Task 1: Upgrade the secondary Management Server

1. Log on to LON-RMS and close the Operations console if it is running.
2. Log on to **LON-MG1**, and then delete the **AgentManagement** folder that is located in C:\Program Files\System Center Operations Manager 2007\.
3. Click **Start**; click **Run**; in the **Run** box, type **\LON-DC1\Media** and then click **OK**.
4. Open the **SCOM2012** folder, and then double-click **Setup.exe** to start Operations Manager setup.
5. In the **Operations Manager** window that opens, click **Install**.
6. In the Operations Manager Setup wizard, on the **Getting Started** page, click **Next**.
7. On the **Select installation location** page, click **Next**.
8. On the **Proceed with Setup** page, click **Next**.
9. On the **Configure Operations Manager accounts** page, select **Domain Account**; in the **Domain\User Name** box, type **Contoso\svc\_SCOM2007\_das**; in the **Password** box, type **Pa\$\$w0rd**; and then click **Next**.
10. On the **Ready to Upgrade** page, click **Upgrade**.
11. On the **Upgrade complete** page, click **Close**.

### ► Task 2: Upgrade the push-installed agents

1. Log on to LON-RMS and open the Operations console.
2. Click the **Administration** pane, and then expand **Device Management**.
3. Click **Pending Management**, and then in the **Details** pane, right-click and then click **Refresh**. Notice that under **Type: Agent Requires Update (1)**, **LON-DC1** is listed.
4. Click **LON-DC1** and then in the **Actions** pane, click **Approve**.
5. In the **Update Agents** window that opens, click **Other user account**; in the **User name** box, type **Administrator**; in the **Password** box, type **Pa\$\$w0rd**; and then click **Update**.
6. In the **Agent Management Task Status** window that opens, under **Task Output**, wait until the **The task completed successfully** message is displayed, and then click **Close**.



**Note:** If the upgrade fails, perform the following steps.

1. In the **Pending Management** view, click **LON-DC1**, and then in the **Actions** pane, click **Reject**.
2. Under **Device Management**, click **Agent Managed**, right-click **LON-DC1**, and then click **Delete**.
3. In the **Confirm Delete Monitoring Agent** window that opens, click **Yes**.

### ► Task 3: Check for any active connected consoles to the RMS

1. On LON-RMS close the Operations console.
2. Click **Start**, click **Administrative Tools**, and then click **Performance Monitor**.
3. In the navigation pane of the Performance Monitor, expand **Monitoring Tools**, and then click **Performance Monitor**.

4. Click the Plus Sign (+) button to add a counter.
5. In the **Add Counters** window that opens, under **Available counters**, scroll down, expand **OpsMgr SDK Service**, click **Client Connections**, click **Add**, and then click **OK**.

The Client Connections are now shown in Performance Monitor.

6. Close Performance Monitor.

#### ► Task 4: Run the Management Group upgrade on the RMS

1. Log on to LON-RMS, and then delete the **AgentManagement** folder that is located in C:\Program Files\System Center Operations Manager 2007\.
2. Close the Operations console if it is open.
3. Click **Start**; click **Run**; in the **Run** box, type **\LON-DC1\Media**; and then click **OK**.
4. Double-click **ReportViewer.exe**.
5. In the **Open File – Security Warning** window that opens, click **Run**.
6. In the **Microsoft ReportViewer 2010 Redistributable Setup** wizard that opens, click **Next**.
7. On the **Welcome to the Microsoft ReportViewer 2010 Redistributable Setup** page, select **I have read and accept the license terms**, and then click **Install**.
8. On the **Installation Is Complete** page, click **Finish**.
9. From **\LON-DC1\Media**, open the **SCOM2012** folder, and then double-click **Setup** to start the Operations Manager setup.
10. In the **Operations Manager** window that opens, click **Install**.
11. In the Operations Manager Setup wizard, on the **System Center 2012 – Operations Manager Upgrade** page, click **Next**.
12. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
13. On the **Select installation location** page, click **Next**.
14. On the **Proceed with Setup** page, click **Next**.
15. On the **Configure Operations Manager accounts** page, select **Domain Account**; in the **Domain\User Name** box for the **System Center Configuration service and System Center Data Access service account**, type **Contoso\svc\_SCOM2007\_das**; in the **Password** box, type **Pa\$\$w0rd**; and then click **Next**.
16. On the **Ready to Upgrade** page, click **Upgrade**.



**Note:** The upgrade process can take up to two hours to complete.

17. On the **Upgrade complete** page, click **Close**.

#### ► Task 5: Verify the success of the upgrade

1. Log on to LON-RMS, click Start, click All Programs\Microsoft System Center 2012\Operations Manager, and then click Operations Console.
2. Click the Monitoring pane, and then expand **Operations Manager Upgrade MP**.
3. Click **Step 4: Upgrade Root Management Server and Databases (Upgrade Helper MP)**, and in the Details pane, confirm that **LON-RMS** is visible and in a healthy state.

**Results:**

After this exercise, you should have performed an upgrade of the existing Operations Manager 2007 R2 environment to System Center 2012 Operations Manager. This includes the secondary Management Server, agents, and RMS. By using the Operations Manager Upgrade Management Pack, you confirmed that the RMS upgraded successfully.

## Exercise 3: Upgrading the System Center 2012 Management Group to System Center 2012 SP1

### ► Task 1: Prepare the System Center 2012 Operations Manager environment

1. Log on to LON-RMS.
2. Click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
3. In the **Connect to Server** window that opens, click **Connect**.
4. In Microsoft SQL Server Management Studio, click **New Query**.
5. From drive C, open the **CheckETL.txt** file, and then copy the contents into the **SQL Query** window.
6. Next to the **Execute** button, click the drop-down list, and then click **OperationsManager**.
7. Click **Execute**, and note the results.
8. Click **New Query**, and then from drive C, open the **CleanETL.txt** file.
9. Copy the contents into the new query window.
10. Next to the **Execute** button, click the drop-down list, and then click **OperationsManager**.
11. Click **Execute**.
12. Wait until the query completes, and then close Microsoft SQL Server Management Studio.
13. In the **Microsoft SQL Server Management Studio** pop-up window that opens, click **No**.
14. Log on to LON-MG1, click **Start**, and then click **Run**.
15. In the **Run** window that opens, in the **Open** box, type **regedit32**, and then click **OK**.
16. In the **Registry Editor** window that opens, browse to  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup**.
17. In the details pane, double-click **DataWarehouseDBName**.
18. In the **Edit String** window that opens, in the **Value data** box, type **OperationsManagerDW**, and then click **OK**.
19. In the details pane, double-click **DataWarehouseDBServerName**.
20. In the **Edit String** window that opens, in the **Value data** box, type **LON-RMS**, and then click **OK**.
21. Close the **Registry Editor** window.

### ► Task 2: Upgrade the first Management Server

1. Restart **LON-MG1**.
2. Log on to LON-MG1, and then browse to **\LON-DC1\Media\SCOM2012SP1**.
3. Double-click **Setup.exe**.
4. In the **Open File – Security Warning** window that opens, click **Run**.
5. In the **System Center 2012** window that opens, click **Install**.
6. In the System Center 2012 – Operations Manager Upgrade wizard that starts, click **Next**.
7. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
8. On the **Select installation location** page, click **Next**.

9. On the **Proceed with Setup** page, click **Next**.
  10. On the **Configure Operations Manager accounts** page, select **Domain Account**, and then in the **Domain\User Name** box, type **Contoso\svc\_SCOM2007\_das**.
  11. In the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
  12. On the **Ready To Upgrade** page, click **Upgrade**.
  13. On the **Setup is complete** page, click **Close**.
- **Task 3: Upgrade the second Management Server**
1. Restart **LON-RMS**.
  2. Log on to LON-RMS, and then browse to **\LON-DC1\Media\SCOM2012SP1**.
  3. Double-click **Setup.exe**.
  4. In the **Open File – Security Warning** window that opens, click **Run**.
  5. In the **System Center 2012** window that opens, click **Install**.
  6. In the System Center 2012 – Operations Manager Upgrade wizard that starts, click **Next**.
  7. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
  8. On the **Select installation location** page, click **Next**.
  9. On the **Proceed with Setup** page, click **Next**.
  10. On the **Configure Operations Manager accounts** page, select **Domain Account**, and then in the **Domain\User Name** box, type **Contoso\svc\_SCOM2007\_das**.
  11. In the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
  12. On the **Ready To Upgrade** page, click **Upgrade**.
  13. On the **Setup is complete** page, click **Close**.
- **Task 4: Verify the success of the upgrade**
1. Log on to LON-RMS, click **Start>All Programs\Microsoft System Center 2012\Operations Manager**, and then click **Operations Console**.
  2. Note on the Operations console loading screen that **System Center 2012 SP1 Operations Manager** is displayed.
  3. In the Operations console, click the **Administration** pane, expand **Device Management**, and then click **Management Servers**.
  4. Confirm that both **LON-RMS** and **LON-MG1** are displayed and are in a healthy state.
  5. Click the **Reporting** pane, and then click **Microsoft ODR Report Library**.
  6. In the details pane, click **Management Group**, and then in the **Tasks** pane, click **Open**.
  7. Confirm the **Management Group ODR Report** opens as expected, and then close the report window.
  8. Close the Operations console.

**Results:** After this exercise, you should have upgraded the Operations Manager Management Group to System Center 2012 SP1 Operations Manager. You should have also confirmed that the Management Group is operating as expected.

## Exercise 4: Upgrading the System Center 2012 SP1 Management Group to System Center 2012 R2 Operations Manager

### ► Task 1: Upgrade the first Management Server

1. Restart **LON-MG1**.
2. Log on to LON-MG1, and then browse to **\LON-DC1\Media\SCOM2012R2**.
3. Double-click **Setup.exe**.
4. In the **Open File – Security Warning** window that opens, click **Run**.
5. In the **System Center 2012 R2** window that opens, click **Install**.
6. In the System Center 2012 R2 Operations Manager Upgrade wizard that starts, click **Next**.
7. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
8. On the **Select installation location** page, click **Next**.
9. On the **Proceed with Setup** page, click **Next**.
10. On the **Configure Operations Manager accounts** page, select **Domain Account**, and in the **Domain\User Name** box, type **Contoso\svc\_SCOM2007\_das**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
12. On the **Ready To Upgrade** page, click **Upgrade**.
13. On the **Setup is complete** page, click **Close**.

 **Note:** Note that the upgrade will complete with a Warning status. This is expected and is related to an evaluation version being installed.

### ► Task 2: Upgrade the second Management Server

1. Restart **LON-RMS**.
2. Log on to LON-RMS, and then browse to **\LON-DC1\Media\**.
3. Double-click **ReportViewer.msi**.
4. In the **Open File – Security Warning** window that opens click **Run**.
5. In the **Microsoft Report Viewer 2012 Runtime** wizard that opens click **Next**.
6. On the **License Agreement** page select the **I accept the terms in the license agreement** check box and then click **Next**.
7. On the **Ready to Install the Program** page click **Install**.
8. On the **Completing the Microsoft Report Viewer 2012 Runtime installation** page click **Finish**.
9. Navigate to **\LON-DC1\Media\SCOM2012R2**.
10. Double-click **Setup.exe**.
11. In the **Open File – Security Warning** window that opens, click **Run**.
12. In the **System Center 2012 R2** window that opens, click **Install**.
13. In the System Center 2012 R2 Operations Manager Upgrade wizard that starts, click **Next**.

14. On the **Please read the license terms** page, select **I have read, understood, and agree with the license terms**, and then click **Next**.
15. On the **Select installation location** page, click **Next**.
16. On the **Proceed with Setup** page, click **Next**.
17. On the **Configure Operations Manager accounts** page, select **Domain Account**, and then in the **Domain\User Name** box, type **Contoso\svc\_SCOM2007\_das**.
18. In the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
19. On the **Ready To Upgrade** page, click **Upgrade**.
20. On the **Setup is complete** page, click **Close**.

► **Task 3: Verify the success of the upgrade**

1. Log on to LON-RMS, click **Start>All Programs\Microsoft System Center 2012\Operations Manager**, and then click **Operations Console**.
2. Note on the Operations console loading screen that **Microsoft System Center 2012 R2** is displayed.
3. In the Operations console, click the **Administration** pane, expand **Device Management**, and then click **Management Servers**.
4. Confirm both **LON-RMS** and **LON-MG1** are displayed and are both in a healthy state.
5. Click the **Reporting** pane, and then click **Microsoft ODR Report Library**.
6. In the details pane, click **Management Group**, and then in the **Tasks** pane, click **Open**.
7. Confirm the **Management Group ODR Report** opens as expected, and then close the report window.
8. Close the Operations console.



**Note:** If either LON-MG1 or LON-RMS appear in a greyed out state in the Operations console, restart LON-RMS and LON-MG1.

**Results:** After this exercise, you should have upgraded the Management Group to System Center 2012 R2 Operations Manager. You should have also confirmed that the upgrade was successful by verifying that the Management Group is operating as expected.

# Module 4: Configuring Fabric and Application Monitoring

## Lab: Configuring Application and Fabric Monitoring

### Exercise 1: Installing the System Center Management Pack for Windows Server Operating System

► Task 1: Install the System Center Management Pack for Windows Server Operating System

1. Log on to LON-MS1, and then open the **Operations console**.
2. Click the **Administration** pane, and then click **Management Packs**.
3. In the **Tasks** pane, click **Import Management Packs**.
4. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
5. In the **Online Catalog Connection** window that opens, click **No**.
6. Browse to **\LON-DC1\Media\Additional Management Packs\Windows Server Operating System\Windows Server 2012 R2**.
7. Select all **.mp** files, and then click **Open**.
8. In the **Import Management Packs** window, click **Install**.
9. Wait for the Management Packs to import, and then click **Close**.

► Task 2: Confirm the operating systems have been discovered and monitored

1. On LON-MS1, in the Operations console, click the Monitoring pane.
2. Expand **Microsoft Windows Server**, and then click **Windows Server State**.
3. Confirm **LON-SQ1.CONTOSO.COM** is displayed in the details pane and is in a healthy state.
4. Expand **Health Monitoring**.
5. Click **Operating System Health**.
6. In the details pane, under **Operating System State**, confirm that **LON-SQ1.CONTOSO.COM** is displayed.
7. Click **LON-SQ1.CONTOSO.COM**, and then review the details in the **Detail View**.
8. In the **Health Monitoring** folder, click **Disk Health**.
9. In the details pane, confirm that Drive **C** for **LON-SQ1.CONTOSO.COM** is visible and in a healthy state.

 **Note:** It may take up to 10 minutes for the Operating System to be discovered.

**Results:** After this exercise, you should have installed the System Center Management Pack for Windows Server Operating System and confirmed that the operating systems have been discovered and are in a healthy state.

## Exercise 2: Installing and Configuring the System Center Management Pack for SQL Server

### ► Task 1: Create a SQL Server monitoring account

1. Log on to LON-DC1, click **Start**, and then click **Administrative Tools**.
2. Double-click **Active Directory Users and Computers**.
3. In **Active Directory Users and Computers**, right-click the **SCOM2012** container, click **New**, and then click **User**.
4. In the New Object – User wizard that opens, in both the **First name** and **User logon name** boxes, type **SQLMonitoring**, and then click **Next**.
5. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**.
6. Clear the **User must change password at next logon** check box, select the **Password never expires** check box, click **Next**, and then click **Finish**.
7. Close **Active directory Users and Computers**, and then log off LON-DC1.

### ► Task 2: Create a Run As account

1. On LON-MS1, in the Operations console, click the **Administration** pane.
2. Expand **Run As Configuration**, and then click **Accounts**.
3. From the **Tasks** pane, click **Create Run As Account**.
4. In the Create Run As Account Wizard that opens, on the **Introduction** page, click **Next**.
5. On the **General Properties** page, under **Run As account type**, ensure **Windows** is selected; in the **Display Name** box, type **SQL Monitoring Account**; and then click **Next**.
6. On the **Credentials** page, in the **User name** box, type **SQLMonitoring**; in both the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**; and then click **Next**.
7. On the **Distribution Security** page, ensure **More secure** is selected, and then click **Create**.
8. On the **Wizard completed successfully** page, click **Close**.
9. In the details pane, right-click **SQL Monitoring Account**, and then click **Properties**.
10. In the **Run As Account Properties – SQL Monitoring Account** window that opens, click the **Distribution** tab, and then click **Add**.
11. In the **Computer Search** window that opens, click **Search**.
12. Under **Available Items**, click **LON-SQ1.CONTOSO.COM**, click **Add**, and then click **OK**.
13. In the **Run As Account Properties – SQL Monitoring Account** window, click **OK**.

### ► Task 3: Create a group

1. On LON-MS1, in the Operations console, click the **Authoring** pane.
2. Right-click **Groups**, and then click **Create a new Group**.
3. In the Create Group Wizard, on the **General Properties** page, in the **Name** box, type **Contoso SQL Servers**.
4. Under **Management pack**, click **New**.
5. In the Create a Management Pack wizard, on the **General Properties** page, in the **Name** box, type **Contoso SQL Servers**, and then click **Next**.

6. On the **Knowledge** page, click **Create**.
7. In the Create Group Wizard, on the **General Properties** page, click **Next**.
8. On the **Explicit Members** page, click **Add/Remove Objects**.
9. In the **Create Group Wizard – Object Selection** window that opens, click the drop-down list, click **Windows Computer**, and then click **Search**.
10. Under **Available items**, click **LON-SQ1.CONTOSO.COM**, click **Add**, and then click **OK**.
11. On the **Explicit Members** page, click **Next**.
12. On the **Dynamic Members** page, click **Next**.
13. On the **Subgroups** page, click **Next**.
14. On the **Excluded Members** page, click **Create**.

► **Task 4: Install the System Center Management Pack for SQL Server**

1. On LON-MS1, in the Operations console, click the **Administration** pane, and then click **Management Packs**.
2. In the **Tasks** pane, click **Import Management Packs**.
3. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
4. In the **Online Catalog Connection** window that opens, click **No**.
5. Browse to **\LON-DC1\Media\Additional Management Packs\SQL Server**
6. Select all **.mp** files, and then click **Open**.
7. In the **Import Management Packs** window, click **Install**.
8. Wait for the Management Packs to import, and then click **Close**.

► **Task 5: Configure the Run As profiles**

1. On LON-MS1, in the Operations console, click the **Administration** pane, expand **Run As Configuration**, and then click **Profiles**.
2. In the details pane, right-click **SQL Server Default Action Account**, and then click **Properties**.
3. In the Run As Profile Wizard, on the **Introduction** page, click **Next**.
4. On the **General Properties** page, click **Next**.
5. On the **Run As Accounts** page, click **Add**.
6. In the **Add a Run As Account** window that opens, under **Run As Account**, click the drop-down list, and then click **SQL Monitoring Account**.
7. Select **A selected class, group or object**, click **Select**, and then click **Group**.
8. In the **Group Search** window that opens, click **Search**.
9. Under **Available Groups**, click **Contoso SQL Servers**, and then click **OK**.
10. In the **Add a Run As Account** window, click **OK**.
11. Click **Save**, and then click **Close**.
12. In the details pane, right-click **SQL Server Discovery Account**, and then click **Properties**.
13. In the Run As Profile Wizard, on the **Introduction** page, click **Next**.
14. On the **General Properties** page, click **Next**.

15. On the **Run As Accounts** page, click **Add**.
16. In the **Add a Run As Account** window that opens, click the **Run As Account**, drop-down list, and then click **SQL Monitoring Account**.
17. Select **A selected class, group or object**, click **Select**, and then click **Group**.
18. In the **Group Search** window that opens, click **Search**.
19. Under **Available Groups**, click **Contoso SQL Servers**, and then click **OK**.
20. In the **Add a Run As Account** window, click **OK**.
21. Click **Save**, and then click **Close**.
22. In the details pane, right-click **SQL Server Monitoring Account**, and then click **Properties**.
23. In the Run As Profile Wizard, on the **Introduction** page, click **Next**.
24. On the **General Properties** page, click **Next**.
25. On the **Run As Accounts** page, click **Add**.
26. In the **Add a Run As Account** window that opens, under **Run As Account**, click the drop-down list, and then click **SQL Monitoring Account**.
27. Select **A selected class, group or object**, and then click **Select**, and then click **Group**.
28. In the **Group Search** window that opens, click **Search**.
29. Under **Available Groups**, click **Contoso SQL Servers**, and then click **OK**.
30. In the **Add a Run As Account** window, Click **OK**.
31. Click **Save**, and then click **Close**.

► **Task 6: Configure permissions on the computer running SQL Server**

1. Logon to LON-SQ1, right-click **Start**, and then click **Computer Management**.
2. In **Computer Management**, expand **Local Users and Groups**, and then click **Groups**.
3. In the details pane, right-click **Administrators**, and then click **Properties**.
4. In the **Administrator Properties** window that opens, click **Add**.
5. In the **Select Users, Computers, Service Accounts, or Groups** window that opens, in the **Enter the object names to select** box, type **SQLMonitoring**, and then click **Check Names**.
6. In the **Select Users, Computers, Service Accounts, or Groups** window, click **OK**.
7. In the **Administrator Properties** window, click **OK**.
8. Close the **Computer Management** window.
9. Log off LON-SQ1.

► **Task 7: Confirm SQL monitoring**

1. On LON-MS1, in the Operations console, click the **Monitoring** pane, expand **Microsoft SQL Server**, expand **Databases**, and then click **Database State**.
2. In the details pane, confirm that all the databases, including the **OperationsManager** and **OperationsManagerDW** databases, are visible and are displaying a healthy state.
3. Expand **SQL Agent**, and then click **SQL Agent State**.
4. In the details pane, confirm the **SQLSERVERAGENT** for **LON-SQ1** is visible and is displaying a healthy state.

5. Expand **Server Roles** and then click **Database Engines** and confirm **LON-SQ1** is displayed in a healthy state.
6. Notice the various **SQL DB Engine Tasks** that are available from the **Tasks** pane.
7. Click **Reporting Services** and confirm **LON-SQ1** is displayed in a healthy state.

 **Note:** It may take up to 15 minutes for the SQL Server components to be discovered. You can continue with the next task before the components are discovered.

**Results:** After this exercise, you should have installed the System Center Management Pack for SQL Server. You will have created a Run As account for discovering SQL Server and associated it with the relevant SQL Server Run As profiles.

## Exercise 3: Installing the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8

### ► Task 1: Install the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, and then click **Management Packs**.
3. In the **Tasks** pane, click **Import Management Packs**.
4. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
5. In the **Online Catalog Connection** window that opens, click **No**.
6. Browse to **\LON-DC1\Media\Additional Management Packs\Internet Information Services 8**.
7. Select all **.mp** files, and then click **Open**.
8. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
9. If the **Online Catalog Connection** window opens, click **No**.
10. Browse to **\LON-DC1\Media\Additional Management Packs\Internet Information Services 7**.
11. Select all **.mp** files except the **Microsoft.Windows.InternetInformationServices.CommonLibrary.mp** file, and then click **Open**.
12. In the **Import Management Packs** window, click **Install**.
13. Wait for the Management Packs to import, and then click **Close**.

### ► Task 2: Confirm IIS monitoring

1. On LON-MS1, in the Operations console, click the **Monitoring** pane, expand **Microsoft Windows Internet Information Services**, and then click **IIS Role State**.
2. In the details pane, confirm the **IIS Role** for LON-AP1, LON-AP2, and LON-MS1 is visible and is displayed in a healthy state.
3. Click **Web Site State**.
4. In the details pane, confirm the **SharePoint – 80, Team Foundation Server** and **SharePoint Central Administration v4** websites are visible and in a healthy state.
5. Click **Application Pool State**, and in the details, confirm the **OperationsManager** and **SharePoint Central Administration v4** application pools are visible and in a healthy state.



**Note:** It may take up to 15 minutes for the IIS components to be discovered.

**Results:** After this exercise, you should have installed the System Center 2012 Management Pack for Microsoft Windows Server 2012 Internet Information Service 8 and confirmed that the web applications were discovered and monitored.

## Exercise 4: Installing and Configuring the System Center Management Pack for SharePoint Server 2013

### ► Task 1: Install the System Center Management Pack for SharePoint Server 2013

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, and then click **Management Packs**.
3. In the **Tasks** pane, click **Import Management Packs**.
4. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
5. In the **Online Catalog Connection** window that opens, click **No**.
6. Browse to **\LON-DC1\Media\Additional Management Packs\SharePoint Server**
7. Select all **.mp** files, and then click **Open**.
8. In the **Import Management Packs** window, click **Install**.
9. Wait for the Management Packs to import, and then click **Close**.

### ► Task 2: Configure the System Center Management Pack for SharePoint Server 2013

1. Log on to LON-MS1, and create a folder named **System Center Management Packs** in the **C:\Program Files** folder.
2. From the **\LON-DC1\Media\Additional Management Packs\SharePoint Server** folder, copy the **Microsoft.SharePoint.foundation.library.mp.config** file to the **C:\Program Files\System Center Management Packs** folder.
3. Open the Operations console, and then click the **Administration** pane.
4. Expand **Run As Configuration**, and then click **Accounts**.
5. From the **Tasks** pane, click **Create Run As Account**.
6. In the Create Run As Account Wizard that opens, on the **Introduction** page, click **Next**.
7. On the **General Properties** page, in the **Display name** box, type **SharePoint Discovery/Monitoring Account**, and then click **Next**.
8. On the **Credentials** page, in the **User name** box, type **Administrator**; in both the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**; and then click **Next**.
9. On the **Distribution Security** page, ensure **More secure** is selected, and then click **Create**.
10. On the **Wizard completed successfully** page, click **Close**.
11. In the details pane, right-click **SharePoint Discovery/Monitoring Account**, and then click **Properties**.
12. In the **Run As Account Properties – SharePoint Discovery/Monitoring Account** window that opens, click the **Distribution** tab.
13. Click **Add**, and then in the **Computer Search** window that opens, click **Search**.
14. Under **Available items**, click **LON-AP1.CONTOSO.COM**, click **Add**, and then click **OK**.
15. In the **Run As Account Properties – SharePoint Discovery/Monitoring Account** window, click **OK**.
16. Click the **Monitoring** pane, expand **Microsoft SharePoint**, and then click **Administration**.
17. In the details pane, click **Microsoft SharePoint Farm Group**.



**Note:** The Microsoft SharePoint Farm Group may be displayed in a **Not monitored** state. This is normal as discovery of all SharePoint resources has not completed yet.

18. In the **Tasks** pane, click **Configure SharePoint Management Pack**.
19. In the **Run Task – Configure SharePoint Management Pack** window that opens, click **Run**.
20. In the **Task Status – Configure SharePoint Management Pack** window that opens, monitor the **Task Output** window until a message stating **SharePoint management pack configuration completed successfully** appears, and then click **Close**.



**Note:** If the task fails, wait for 5 minutes and then run the task again. This is due to SharePoint objects being discovered.

#### ► **Task 3: Confirm SharePoint monitoring**

1. On LON-MS1, in the Operations console, click the **Monitoring** pane.
2. Expand **Microsoft SharePoint**, and then click **Servers**.
3. When **LON-API.CONTOSO.COM** appears, which can take up to 10 minutes, click the **Service Front Ends** view, and then confirm the **Access Page**, **Access Page 2013** and **Excel Services Application Page** components are visible.



**Note:** Some components may be in a warning or critical state. This is expected and confirms that the SharePoint Management Pack is monitoring SharePoint.

4. Click the **Shared Services** view, and review the shared services that have been discovered.
5. Click the **Diagram View**, and review the diagram that has been created for the various SharePoint Server 2013 components.
6. Click the **Web Applications** view, and review the **SharePoint – 80** and **SharePoint Central Administration v4** websites that have been discovered.



**Note:** It can take up to 30 minutes for all SharePoint components to be discovered.

**Note:** Some websites may be in a warning or critical state. This is expected and confirms that the SharePoint Management Pack is monitoring SharePoint.

**Results:** After this exercise, you should have installed and configured the System Center Management Pack for SharePoint Server 2013. You should also have confirmed that Operations Manager discovered the SharePoint environment and monitored the various components of SharePoint Server 2013.

## Exercise 5: Configuring Network Monitoring

### ► Task 1: Configure IP addresses on LON-AP2

1. On LON-AP2, click **Start**, click **Control Panel** and then in the **All Control Panel Items** window that opens click **Network and Sharing Center**.
2. Click **Change adapter settings** then right-click **Local Area Connection 2** and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
4. Click **Advanced** and then in the **Advanced TCP/IP Settings** window that opens, under **IP addresses** click **Add**.
5. In the **TCP/IP Address** window that opens type **10.10.0.35** in the **IP address** box and then press tab on the keyboard and then click **Add**.
6. Under **IP Addresses**, click **Add** again.
7. In the **TCP/IP Address** window that opens type **10.10.0.36** in the **IP address** box and then press tab on the keyboard and then click **Add**.
8. Under **IP Addresses**, click **Add** again.
9. In the **TCP/IP Address** window that opens type **10.10.0.37** in the **IP address** box and then press tab on the keyboard and then click **Add**.
10. Click **OK** on the **Advanced TCP/IP Settings** window.
11. Click **OK** on the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.
12. Click **Close** on the **Local Area Connection 2 Properties** window.
13. Close the **Network Connections** window.
14. Log off LON-AP2.

### ► Task 2: Install the SNMP Device Simulator

1. Logon to LON-AP2.
2. Open the **C:\Jalasoft** folder, right-click **SNMPDeviceSimulator5.0.zip**, and then click **Extract All**.
3. In the **Extract Compressed (Zipped) Folders** window that opens, click **Extract**.
4. Open the **C:\Jalasoft\SNMPDeviceSimulator5.0\SNMP Device Simulator 5.0.304.ORTM** folder, and then double-click **Setup.exe**.
5. If the Open File – Security Warning window opens, click Run.
6. In the **Welcome to the Jalasoft Xian SNMP Device Simulator v5 Installer Wizard** that opens, click **Next**.
7. On the **End-User License Agreement** page, **select I accept the terms in the License Agreement**, and then click **Next**.
8. On the **Features** page, click **Next**.
9. On the **Agent service parameters** page, in the **IP address** drop-down list, make sure that **10.10.0.35** is selected, and then click **Next**.
10. On the **Ready to Install** page, click **Install**.
11. On the **The Jalasoft Xian SNMP Device Simulator v5 has been successfully installed** page, click **Finish**.

► **Task 3: Configure the SNMP Device Simulator**

1. From the desktop, double-click **Xian SNMP Device Simulator v5 Console**.
2. In the **Add Agent** window that opens, click **Add**.
3. In the **Xian SNMP Device Simulator v5 Console** window that opens, right-click **10.10.0.35:9090**, and then click **Simulate Device**.
4. In the **Simulate Device** window that opens, on the **Device** tab, in the **Model** section, click **3Com Switch 3900-24**, and then click **Next**.
5. On the **IP Address** tab, select **10.10.0.36**, and then click **Next**.
6. On the **SNMP settings** tab, click **Finish**.
7. Right-click **10.10.0.35:9090**, and then click **Simulate Device**.
8. In the **Simulate Device** window that opens, on the **Device** tab, in the **Model** section, click **Cisco PIX 520 Firewall**, and then click **Next**.
9. On the **IP Address** tab, select **10.10.0.37**, and then click **Next**.
10. On the **SNMP settings** tab, click **Finish**.
11. Close the **Xian SNMP Device Simulator v5 Console** window, and then log off LON-AP2.

► **Task 4: Discover the network devices**

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, expand **Network Management**, and then click **Discovery Rules**.
3. In the **Tasks** pane, click **Discover Network Devices**.
4. In the Network Devices Discovery Wizard that opens, on the **General Properties** page, in the **Name** box, type **Contoso**; in the **Available servers** drop-down list, click **LON-MS1.CONTOSO.COM**; and then click **Next**.
5. On the **Discovery Method** page, make sure that **Explicit discovery** is selected, and then click **Next**.
6. On the **Default Accounts** page, click **Create Account**.
7. In the **Create Run As Account Wizard**, on the **Introduction** page, click **Next**.
8. On the **General Properties** page, in the **Display name** text box, type **Contoso**; and then click **Next**.
9. On the **Credentials** page, in the **Community string** box, type **public**, and then click **Create**.
10. On the **Default Accounts** page, click **Next**.
11. On the **Devices** page, click **Add**.
12. In the **Add a Device** window that opens, in the **Name or IP address** box, type **3Com-3900-24**, and then click **OK**.
13. On the **Devices** page, click **Next**.
14. On the **Schedule Discovery** page, select **Run the discovery manually**, and then click **Next**.
15. On the **Summary** page, click **Create**.
16. In the **Warning** pop-up window that opens, click **Yes**.
17. On the **Completion** page, make sure that the **Run this network discovery rule after the wizard is closed** option is clicked, and then click **Close**.

18. In the **Tasks** pane, click **Refresh** periodically to monitor the **Last Discovered** column until it changes from **0** to **1**.



**Note:** It can take up to five minutes for the network devices to be discovered.

19. Under **Network Management**, click **Network Devices**, and then confirm the network device has been discovered.
20. On the **Details** pane, periodically right-click in the white space area and then click **Refresh** until the **10.10.0.36** device is displayed.

This should take no longer than five minutes.

21. Click **Discovery Rules** and then right-click the **Contoso** rule and then click **Properties**.
22. In the **Network Devices Discovery Wizard**, on the **General Properties** page click **Next**.
23. On the **Discovery Method** page click **Next**.
24. On the **Default Accounts** page click **Next**.
25. On the **Devices** page click **3Com-3900-24** and then click **Edit**.
26. In the **Device Settings** window that opens remove **3Com-3900-24** from the **Name or IP address** box and then type **CiscoPix-520** then click **OK**.
27. Click **Next** on the **Devices** page.
28. On the **Schedule Discovery** page click **Next**.
29. On the **Summary** page click **Save**.
30. On the **Completion** page ensure the **Run the network discovery rule after the wizard is closed** check box is selected and then click **Close**.
31. Click the **Network Devices** view and wait until the **10.10.0.37** device is displayed.
32. Click the **Monitoring** pane, and then expand **Network Monitoring**.
33. Click **Switches**, and then notice from the **Model** column that the **SuperStack-3900-24** switch has been discovered.
34. Review the information in the **Detail view**.
35. Click **Routers**, and then notice from the **Model** column that the **PIX Firewall 525** firewall has been discovered.
36. Review the information in the **Detail view**.

#### ► Task 5: Simulate a network device failure

1. Log on to LON-AP2, click **Start**, and then click **Control Panel**.
2. Click **Network and Sharing Center**, and in the **Network and Sharing Center** window that opens, click **Change Adapter Settings**.
3. In the **Network Connections** window that opens, right-click **Local Area Connection 2**, and then click **Properties**.
4. In the **Local Area Connection 2 Properties** window that opens, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window that opens, click **Advanced**.

6. In the **Advanced TCP/IP Settings** window that opens, under **IP addresses**, click **10.10.0.36**, and then click **Remove**.
7. In the **Advanced TCP/IP Settings** window, click **OK**.
8. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, click **OK**.
9. In the **Local Area Connection 2 Properties** window, click **Close**.

► **Task 6: View the network device Failure alerts in Operations Manager**

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Monitoring** pane, and then click **Active Alerts**.
3. Double-click the **Network Device is Not Responding** alert that is generated.

 **Note:** It can take about five minutes for the alert to appear.

4. On the **General** tab, view the **Alert Description** that shows that the **10.10.0.36** device is not responding.
5. Close the **Alert Properties** window, expand the **Network Monitoring** folder, and then click **Network Devices**.
6. Right-click in the **Details** pane, and then click **Refresh**.

Notice that the **SuperStack 3900-24** network device is in a critical condition.

7. Click **Network Summary Dashboard**; in the **Details** pane, click any node that is in a **Critical** state; and in the **Tasks** pane, click **Network Node Dashboard**.
8. View the details in the **Network Node Dashboard**, including **Average Availability, Instance Details, Average Response Time**, and **Active Alerts Generated by this node**.
9. Log on to LON-AP2, and insert the **10.10.0.36** IP address back into the **Local Area Connection 2** properties.

After about five minutes, the **SuperStack 3900-24** network device will return to a healthy state.

**Results:** After this exercise, you should have configured Network Discovery Rules to discover the network devices that are being simulated on LON-AP2. You should also have simulated a network device failure by removing the IP address details for one of the network devices, and viewed the alert details that Operations Manager generates.

## Exercise 6: Configuring Integration Between Operations Manager and Virtual Machine Manager

► Task 1: Install an Operations Manager agent on the Virtual Machine Manager server and the Hyper-V host

1. On LON-MS1, in the Operations console, click the **Administration** pane, and then click **Discovery Wizard**.
2. In the Computer and Device Management Wizard, on the **Discovery Type** page, click **Next**.
3. On the **Auto or Advanced** page, ensure **Advanced Discovery** is selected, click the **Management Server** drop-down list, click **LON-MS1.CONTOSO.COM**, and then click **Next**.
4. On the **Discovery Method** page, select **Browse for, or type-in computer names**; in the box, type **LON-SC1, LON-HOST1, LON-HOST2** and then click **Next**.

 **Note:** If the host computer names are different than listed above, substitute LON-HOST1 and LON-HOST2 with the host computer names as configured in the lab environment.

5. On the **Administrator Account** page, select **Other user account**; in the **User name** box, type **Administrator**; in the **Password** box, type **Pa\$\$wOrd**; and then click **Discover**.
6. On the **Select Objects to Manage** page, select **LON-SC1.CONTOSO.COM, LON-HOST1.CONTOSO.COM and LON-HOST2.CONTOSO.COM** and then click **Next**.
7. On the **Summary** page, click **Finish**.
8. Wait for the installation to complete, and in the **Agent Management Task Status** window, click **Close**.

► Task 2: Enable Agent Proxying

1. On LON-MS1, in the Operations console click the **Administration** pane and then expand **Device Management** and then click **Agent Managed**.
2. From the details pane right-click **LON-HOST1** and then click **Properties**.
3. In the **LON-HOST1.CONTOSO.COM – Agent Properties** window that opens, click the **Security** tab.
4. Select the check box for **Allow this agent to act as a proxy and discover managed objects on other computers** and then click **OK**.
5. From the details pane right-click **LON-HOST2** and then click **Properties**.
6. In the **LON-HOST2.CONTOSO.COM – Agent Properties** window that opens, click the **Security** tab.
7. Select the check box for **Allow this agent to act as a proxy and discover managed objects on other computers** and then click **OK**.
8. From the details pane right-click **LON-SC1** and then click **Properties**.
9. In the **LON-SC1.CONTOSO.COM – Agent Properties** window that opens, click the **Security** tab.
10. Select the check box for **Allow this agent to act as a proxy and discover managed objects on other computers** and then click **OK**.

► Task 3: Install the Operations console on the Virtual Machine Manager server

1. Log on to LON-SC1, browse to **\LON-DC1\Media\SCOM2012R2**, and then double-click **Setup**.
2. If the Open File – Security Warning window opens, click Run.

3. In the **Operations Manager** window that opens, click **Install**.
4. In the Operations Manager Setup wizard, on the **Select features to install** page, select only **Operations Console**, and then click **Next**.
5. On the **Select installation location** page, click **Next**.
6. On the **Proceed with Setup** page, click **Next**.
7. On the **Please read the license terms** page, select **I have read, understood and agree with the license terms**, and then click **Next**.
8. On the **Help improve Operations Manager** page, select **No I am not willing to participate** in both sections, and then click **Next**.
9. On the **Microsoft Update** page, select **Off**, and then click **Next**.
10. On the **Installation Summary** page, click **Install**.
11. On the **Setup is complete** page, click **Close**.
12. In the **Connect To Server** window that opens, in the **Server name** box, type **LON-MS1**, and then click **Connect**.
13. Confirm that the Operations console opens as expected, and then close the Operations console.
14. Close the **Operations Manager** window.

► **Task 4: Configure the Operations Manager connection in Virtual Machine Manager**

1. Log on to LON-SC1, and on the desktop, double-click **Virtual Machine Manager Console**.
2. In the Virtual Machine Manager console, click the **Settings** pane, and then click **System Center Settings**.
3. In the **Details** pane, double-click **Operations Manager Server**.
4. In the Add Operations Manager wizard that opens, on the **Introduction** page, click **Next**.
5. On the **Connection to Operations Manager** page, in the **Server name** box, type **LON-MS1**, and then select **Use a Run As account**.
6. Click **Browse**; in the **Select a Run As Account** window that opens, click **Administrator**; and then click **OK**.
7. On the **Connection to Operations Manager** page, click **Next**.
8. On the **Connection to VMM** page, in the **User name** box, type **Contoso\Administrator**; in the **Password** box, type **Pa\$\$w0rd**; and then click **Next**.
9. On the **Summary** page, click **Finish**.
10. In the **Jobs** window that opens, monitor the **New Operations Manager connection** job until it completes with a status of **Completed**, and then close the **Jobs** window.

 **Note:** It can take up to 15 minutes for the **New Operations Manager connection** job to complete.

11. Click the **VMs and Services** pane and then under **All Hosts** click **lon-host1**.
12. From the details pane, right-click **10964C-LON-DC1** and then click **Properties**.
13. In the **10964C-LON-DC1 Properties** window that opens, on the **General** tab click the drop-down list next to **Cloud** and then click **Contoso**.

14. Click **OK** on the **10964C-LON-DC1 Properties** window
15. Close the Virtual Machine Manager console.

► **Task 5: Confirm Virtual Machine Manager monitoring**

1. On LON-MS1, in the Operations console, click the **Monitoring** pane, and then expand **Microsoft System Center Virtual Machine Manager**.
2. Expand **Managed Resources**, and then click **Host Health**.
3. Review the **Host State** and **Host Active Alerts** sections, and confirm that the Hyper-V Hosts are displayed.



**Note:** It can take up to 15 minutes for all Virtual Machine Manager resources to be discovered in Operations Manager.

4. Click the **Virtual Machine Health** view, and review the virtual Machines managed by VMM.
5. Click the **Virtual Machine Manager Server Health** view, and review the **Virtual Machine Manager Server State** and **Virtual Machine Manager Server Alerts** sections.
6. Expand **Microsoft System Center Virtual Machine Manager Views**, and then click **Diagram View for LON2DSC1**.
7. Review the Virtual Machine Manager components in the diagram.

**Results:** After this exercise, you should have configured integration between Operations Manager and Virtual Machine Manager.

## Exercise 7: Using the System Center Management Pack for VMM Fabric Dashboard 2012 R2

### ► Task 1: Confirm the Virtual Machine Manager fabric is being monitored

1. On LON-MS1, and in the Operations console, click the **Monitoring** pane, and then expand **Microsoft System Center Virtual Machine Manager**.
2. Expand **Cloud Health Dashboard**, and then click **Cloud Health**.
3. In the details pane, confirm the private clouds have been discovered and are in a healthy state.

 **Note:** If a message stating The **Dashboard view has been deleted or no longer exists** appears then close the Operations console and then re-open it.

4. Click **Contoso** Private Cloud, and then in the **Tasks** pane, click **Fabric Health Dashboard**.
5. Review the information in the **Fabric Health Dashboard**, and then close the **Fabric Health Dashboard**.

 **Note:** The **Fabric Health Dashboard** will not display any data until all VMM resources have been discovered but you can review the data that will be displayed when discovery has completed.

6. Expand **Microsoft System Center Virtual Machine Manager Views**, and then click **Diagram View for LON2DSC1**.
7. In the diagram view, expand **Managed Resources**, and review the Virtual Machine Manager Fabric resources that are being monitored.

**Results:** After this exercise, you should have used the System Center Management Pack for VMM Fabric Dashboard 2012 R2 to confirm that the relevant Virtual Machine Manager fabric resources are discovered and monitored in Operations Manager.

# Module 5: Application Performance Monitoring

## Lab: Monitoring .NET Framework Applications

### Exercise 1: Monitoring .NET Applications

#### ► Task 1: Import the APM Management Pack for IIS

1. Log on to LON-MS1 and Open the Operations console, and then click the **Administration** pane.
2. Click **Management Packs**, and then in the **Tasks** pane, click **Import Management Packs**.
3. In the **Import Management Packs** window that opens, click **Add**, and then click **Add from Disk**.
4. In the **Online Catalog Connection** window that opens, click **No**.
5. In the **Select Management Packs to import** window type **\LON-DC1\Media\SCOM2012R2\ManagementPacks** in the Open box and then press Enter.
6. Click **Microsoft.SystemCenter.Apm.Web.IIS7.mp**, and then click **Open**.
7. Click **Install**, and when the installation is complete, click **Close**.

#### ► Task 2: Configure application performance monitoring

1. Log on to LON-MS1 and then open the Operations console.
2. Click the **Authoring** pane, expand **Management Pack Templates**, and then click **.NET Application Performance Monitoring**.
3. In the **Tasks** pane, click **Add Monitoring Wizard**.
4. In the **Add Monitoring Wizard**, on the **Monitoring Type** page, click **.NET Application Performance Monitoring**, and then click **Next**.
5. On the **General Properties** page, in the **Name** box, type **DinnerNow**, and then next to the **Management pack** drop-down list, click **New**.
6. In the **Create a Management Pack** wizard that opens, on the **General Properties** page type **DinnerNow** in the **Name** box and then click **Next**.
7. On the **Knowledge** page click **Create**.
8. On the **General Properties** page of the **Add Monitoring Wizard**, click **Next**.
9. On the **What to Monitor** page, click **Add**, and then in the **Object Search** window that opens, click **Search**.
10. Under **Available items**, click **DinnerNow**, click **Add**, and then click **OK**.



**Note:** Do not click DinnerNow/Service.

11. Click the **Monitoring scope** drop-down list, click **Production**, and then click **Next**.
12. On the **Server-Side Configuration** page, in the **Performance event threshold (ms)** box, remove **15000**, and then type **50**.
13. Select **Enable additional configuration options for server-side and client-side monitoring**, and then click **Next**.

14. On the **Server-Side Customization** page, click **Customize**.
15. In the **Modify Settings: DinnerNow** window that opens, under **Configure exception event monitoring**, select **Application failure alerts**, and then **All exceptions**.
16. Under **Monitors**, in the **Threshold** box for **% Exception Events/sec exceeds threshold**, remove **15**, and then type **1**.
17. In the **Threshold** box for **% Performance Events/sec exceeds threshold**, remove **20**, and then type **1**.
18. In the **Threshold** box for **Average Request Time exceeds threshold**, remove **10000**, and then type **10**.
19. In the **Modify Settings: DinnerNow** window, click **OK**.
20. On the **Server-Side Customization** page, click **Next**.
21. On the **Client-Side Configuration** page, under **Event monitoring**, select **Turn on exception events alerts**.
22. In the **Page load threshold (ms)** box, remove **15000**, and then type **5**.
23. In the **Ajax and WCF threshold (ms)** box, remove **5000**, and then type **5**.
24. Under **Configure client IP address filter**, click the **Remove** button two times to remove both filters.
25. Click **Advanced Settings**.
26. In the **Advanced Settings: Default for DinnerNow** window that opens, under **Configure performance event collection**, in the **Sensitivity threshold (ms)** box, remove **3000**, and then type **5**.
27. Scroll down, and then under **Monitors**, in the **Threshold** box for **% Exception Events/sec exceeds threshold**, remove **15**, and then type **1**.
28. In the **Threshold** box for **% Performance Events/sec exceeds threshold**, remove **20**, and then type **1**.
29. In the **Threshold** box for **Average Request Time exceeds threshold**, remove **10000**, and then type **10**.
30. In the **Advanced Settings: Default for DinnerNow** window, click **OK**.
31. On the **Client-Side Configuration** page, click **Next**.
32. On the **Enable Client-Side Monitoring** page, for the **DinnerNow** component, select **Enabled**, and then click **Next**.
33. On the **Summary** page, click **Create**.

► **Task 3: Restart IIS**

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Monitoring** pane, and expand the **Operations Manager** folder.
3. Expand **APM Agent Details**, and then click **IIS Restart / Recycle Required**.
4. From the **Details** pane, under **IIS Restart**, click **LON-AP2**, and then in the **Tasks** pane, click **Restart Internet Information Services**.



**Note:** It can take about five minutes for LON-AP2 to appear.

5. In the **Run Task – Restart Internet Information Services** window that opens, click **Run**.
  6. In the **Task Status – Restart Internet Information Services** window that opens click **Close**.
- **Task 4: Browse the DinnerNow website and view application performance alerts**
1. Log on to LON-AP2 and start Windows Internet Explorer.
  2. Browse to <http://LON-AP2/DinnerNow>.
  3. On the **DinnerNow** webpage, in the **Your Zip** box, type **98101**, and then click **Find**.
  4. Click **Northwind Bar & Grill**, and from the list of returned items, next to **Item # 1 Mango Smoothie**, click the **Select** button.
  5. Notice the item is added to the shopping cart.
  6. Next to Item # 2 Sweet Pudin, click Select.
  7. Notice the item does not get added to the shopping cart and a script error is generated.
  8. In the **Windows Internet Explorer** window that opens, click **Close**.
  9. Logon to LON-MS1 and Open the Operations console, and click the **Monitoring** pane.
  10. Expand **Application Monitoring**, expand **.Net Monitoring**, and then click **Active Alerts**.
  11. In the **Details** pane, double-click one of the generated **Server Performance Exception** alerts.
  12. In the **Alert Properties** window, on the **General** tab, click the hyperlink that has been added to the alert description.
  13. In the **Windows Internet Explorer** pop-up window that opens, click **Yes**.
  14. In the **Application Diagnostics** Web console window that opens, notice the custom handler that caused the alert to start based on the threshold breach.
  15. Click the **Performance Counters** tab, and then click the **Diagram View** and **Table View** buttons to view the collected performance counter information.
  16. Close the **Application Diagnostics** Web console.
  17. Close the **Alert Properties** window.
- **Task 5: Simulate a database failure in DinnerNow and view application performance alerts**
1. Log on to LON-AP2 and from the desktop, double-click **DinnerNow SQL DB Detacher**.
  2. In the **SQL Stop Start** window that opens, click **Stop**.
  3. Log on to LON-MS1, and then start Internet Explorer.
  4. Browse to <http://LON-AP2/DinnerNow>.
- Notice that the **Food Type** and **Meal** drop-down menus are empty because the **DinnerNow** database is detached.
5. On LON-MS1, open the Operations console, and then click the **Monitoring** pane.
  6. Expand **Application Monitoring**, expand **.NET Monitoring**, and then click **Active Alerts**.
  7. Refresh the **Active Alerts** view, and notice the **Server Application Exception** alerts that are generated.
  8. View the **Alert Details** pane, and then double-click an alert that includes **Cannot open database** in the description.

9. In the **Alert Properties** window that opens, click the hyperlink that is added to the **Alert Description** to open the Application Diagnostics console.
10. If the **Windows Internet Explorer** window opens, click **Yes**.
11. View the details on the **Event properties** tab to determine the cause of the failure.
12. Click the **Related events** tab and notice the events that are related to this event, such as a **500 Internal Server Error**.
13. Click the **Performance counters** tabs and view the performance counter data that is collected.
14. Close the Application Diagnostics Web console, and then exit Internet Explorer.
15. Close the **Alert Properties** window.
16. On LON-AP2, in the **SQL Stop Start** window, click **Start** to reattach the **DinnerNow** database.
17. Close the **SQL Stop Start** window.

► **Task 6: Use Application Advisor to view application performance monitoring reports**

1. Log on to LON-MS1 and start Internet Explorer.
2. Browse to <http://LON-MS1/AppAdvisor>.
3. In the **Application Advisor** Web console, under **Select report**, click **Application Failure Analysis**.
4. In the lower left pane, scroll down, click to open the **Source** drop-down list, select **DinnerNow – Production**, and then click **Apply**.
5. View the **Application Failure Analysis** report, including the **Failure Breakdown by Resources** and **Top 5 Failures**.
6. Close the **Application Advisor** Web console.

**Results:** After this exercise, you should have configured Application Performance Monitoring for the DinnerNow .NET application, including monitoring the application from both the server-side and the client-side. You should have also used the Application Diagnostics and Application Advisor consoles to view exception and performance data for the application.

## Exercise 2: Configuring IntelliTrace

### ► Task 1: Create a network file share to store IntelliTrace logs

1. On LON-MS1, create a folder named **Alert\_Attachments** on Drive C.
2. Share the folder with **Everyone**, and assign **Read/Write** access to the share.

### ► Task 2: Create a Run As account

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, expand **Run As Configuration**, and then click **Accounts**.
3. In the **Tasks** pane, click **Create Run As Account**.
4. In the Create Run As Account Wizard that starts, on the **Introduction** page, click **Next**.
5. On the **General Properties** page, in the **Display name** box, type **Alert Attachment Account**, and then click **Next**.
6. On the **Credentials** page, in the **User name** box, type **Administrator**
7. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, and then click **Next**.
8. On the **Distribution Security** page, ensure **More secure** is selected, and then click **Create**.
9. On the **Wizard completed** successfully page, click **Close**.
10. In the details pane, right-click **Alert Attachment Account**, and then click **Properties**.
11. In the **Run As Account Properties - Alert Attachment Account** window that opens, click the **Distribution** tab.
12. Click **Add**, and then in the **Computer Search** window that opens, click **Search**.
13. Under **Available items**, click **LON-MS1.CONTOSO.COM**, and click **Add**, and then click **OK**.
14. In the **Run As Account Properties - Alert Attachment Account** window, click **OK**.

### ► Task 3: Import the Alert Attachment Management Pack

1. On LON-MS1, in the Operations console, click in the **Administration** pane, and then click **Management Packs**.
2. In the **Tasks** pane, click **Import Management Packs**.
3. In the **Import Management Packs** window that opens, click **Add**, and then click **Add from disk**.
4. In the **Online Catalog Connection** window that opens, click **No**.
5. In the **Select Management Packs to import** window that opens, type **\LON-DC1\Media\SCOM2012R2\Management Packs**, and then press Enter on the keyboard.
6. Click **Microsoft.SystemCenter.AlertAttachment.mpb**, and then click **Open**.
7. In the **Import Management Packs** window, click **Install**.
8. After the installation has completed, click **Close**.

### ► Task 4: Configure the Alert Attachment Management Pack

1. On LON-MS1, in the Operations console, click the **Administration** pane, and then expand **Run As Configuration**.
2. Click **Profiles**, and from the details pane, right-click **Alert Attachment Management Account**, and then click **Properties**.

3. In the Run As Profile Wizard that starts, on the **Introduction** page, click **Next**.
  4. On the **General Properties** page, click **Next**.
  5. On the **Run As Account** page, click **Add**.
  6. In the **Add a Run As Account** window that opens, click the **Run As Account** drop-down list, click **Alert Attachment Account**, and then click **OK**.
  7. On the **Run As Account** page, click **Save**.
  8. On the **Wizard completed successfully** page, click **Close**.
  9. Click **Authoring**, and then expand **Management Pack Objects**.
  10. Click **Object Discoveries**, and then in the details pane, click **Change Scope**.
  11. In the **Scope Management Pack Objects** window that opens, click **Clear All**, if it is available.
  12. Click **View all targets**, and then in the **Look for** box, type **alert**.
  13. Select **Alert Attachment File Share**, and then click **OK**.
  14. In the details pane, right-click **Alert attachment file share discovery**, and then click **Overrides**.
  15. Click **Override the Object Discovery**, and then click **For all objects of class: Collection Server**.
  16. In the **Override Properties** window that opens, for **Enabled**, select the **Override** check box, and then change the **Override Value** to **True**.
  17. For **Path to the alert attachment file share**, select the **Override** check box; in the **Override Value** box, type **\LON-MS1\Alert\_Attachments**; and then under **Management Pack**, click **New**.
  18. In the Create a Management Pack wizard that starts, in the **Name** box, type **Alert Attachment Management Pack Overrides**, and then click **Next**.
  19. On the **Knowledge** page, click **Create**.
  20. In the **Override Properties** window, click **OK**.
- **Task 5: Import the IntelliTrace Profiling Management Pack**
1. On LON-MS1, in the Operations console, click in the **Administration** pane, and then click **Management Packs**.
  2. In the **Tasks** pane, click **Import Management Packs**.
  3. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
  4. In the **Online Catalog Connection** window that opens, click **No**.
  5. In the **Select Management Packs to import** window that opens, type **\LON-DC1\Media\SCOM2012R2\Management Packs**, and then press Enter.
  6. Click **Microsoft.SystemCenter.IntelliTraceProfiling.mpb**, and then click **Open**.
  7. In the **Import Management Packs** window, click **Install**.
  8. After the installation has completed, click **Close**.
  9. Close the Operations console.
  10. Open the Operations console.
  11. Click the **Monitoring** pane and then expand **IntelliTrace Profiling** and then click **State**.
  12. From the details pane wait until **LON-MS1.CONTOSO.COM** is displayed and the **State** column for **LON-MS1.CONTOSO.COM** displays **Healthy**.

► **Task 6: Collect IntelliTrace profiling snapshots**

1. On LON-MS1, in the Operations console, click the **Monitoring** pane, and then expand **Application Monitoring**.
2. Expand **.NET Monitoring**, and then click **Active Alerts**.
3. From the details pane, click a **Server Performance Exception** alert, note the date and time of the alert as displayed in the **Created** column and then from the **Tasks** pane, click **Start IntelliTrace Collection**.

 **Note:** It is important that you note the date and time of the selected alert in Step 3 as it must be the same alert that is selected later in this exercise.

4. In the **Run Task – Start IntelliTrace** window that opens, click **Run**.
5. In the **Task Status – Start IntelliTrace** window that opens, wait until the task completes, and then click **Close**.
6. Logon to LON-AP2 and Start Internet Explorer, and then browse to <http://lon-ap2/DinnerNow>.
7. In the **DinnerNow** page that opens, in the **Your Zip** box, type **98101**, and then click **Find**.
8. Click **Northwind Bar and Grill**.
9. Next to **Item # 1**, click the **Select** button.
10. Next to **Item # 0**, click the **Select** button.
11. In the **Internet Explorer** popup window that opens, click **Close**.
12. Exit **Internet Explorer**.
13. In the Operations console on LON-MS1, ensure the same alert is selected as noted in Step 3 and then from the **Tasks** pane, click **Collect IntelliTrace Snapshot**.
14. In the **Run Task – Collect IntelliTrace Snapshot** window that opens, click **Run**.
15. In the **Task Status – Collect IntelliTrace Snapshot** window that opens, wait until the task completes, and then click **Close**.
16. In the **Tasks** pane, click **Stop IntelliTrace Collection**.
17. In the **Run Task – Stop IntelliTrace** window that opens, click **Run**.
18. In the **Task Status – Stop IntelliTrace** window that opens, wait for the task to complete, and then click **Close**.
19. Ensure the same alert is selected as noted in Step 3 and then from the **Tasks** pane click **Open Attachment Location**.
20. In the **Windows Explorer** window that opens, open the **DefaultAppPool** folder and confirm the **.iTrace** trace file exists.

► **Task 7: View IntelliTrace snapshots in Visual Studio**

1. On LON-AP1, click **Start**, and then click **Visual Studio 2013**.
2. If a **Microsoft Visual Studio** window opens click **No**.
3. In the **Start Page - Microsoft Visual Studio (Administrator)** window that opens, click the **File** menu, click **Open**, and then click **File**.
4. In the **Open File** window that opens, in the **File name** box, type **\\\LON-MS1**, and then press Enter.

5. Open the **Alert\_Attachments** folder, open the subfolder, and then open the **DefaultAppPool** folder.
6. Click the file that has **the IntelliTrace File type** association, and then click **Open**.
7. In the **IntelliTrace Summary** window that opens, review the IntelliTrace data that has been collected in the following sections:
  - **Exception data**
  - **Web Requests**
  - **System Info**
  - **Threads List**
  - **Modules**

**Results:** After this exercise, you should have installed and configured the Alert Attachment Management Pack and then installed the IntelliTrace Profiling Management Pack. You should also have used the Operations console to start IntelliTrace logging and collected an IntelliTrace log from the .NET web application server.

## Exercise 3: Configuring TFS Integration

### ► Task 1: Import the TFS Work Item Synchronization Management Pack

1. On LON-MS1, in the Operations console, click the **Administration** pane, and then click **Management Packs**.
2. In the **Tasks** pane, click **Import Management Packs**.
3. In the **Import Management Packs** window that opens, click **Add**, and then click **Add from disk**.
4. In the **Online Catalog Connection** window that opens, click **No**.
5. In the **Select Management Packs to import** window that opens, type **\LON-DC1\Media\SCOM2012R2\Management Packs**, and then press Enter.
6. Click **Microsoft.SystemCenter.TFSWISynchronization.mpb**, and then click **Open**.
7. In the **Import Management Packs** window, click **Install**.
8. After the installation has completed, click **Close**.

### ► Task 2: Configure the TFS Work Item Synchronization Management Pack template

1. On LON-MS1, in the Operations console, click the **Authoring** pane, and then expand **Management Pack Templates**.
2. Click **TFS work Item Synchronization**, and then in the **Tasks** pane, click **Add Monitoring Wizard**.
3. In the Add Monitoring Wizard that starts, on the **Monitoring Type** page, click **TFS Work Item Synchronization**, and then click **Next**.
4. On the **General Properties** page, in the **Name** box, type **Contoso TFS Environment**, and then under **Management pack**, click **New**.
5. In the **Create a Management Pack** wizard that starts, on the **General Properties** page, in the **Name** box, type **Contoso TFS Management Pack**, and then click **Next**.
6. On the **Knowledge** page, click **Create**.
7. On the **General Properties** page, click **Next**.
8. On the **Server Settings** page, in the **Team Project Collection URL** box, type **http://lon-ap1:8080/tfs/Contoso/**.
9. Click Create Resource Pool and in the Create a Resource Pool Wizard that opens, on the General Properties page type LON-MS2 in the Name box and then click Next.
10. On the **Pool Membership** page click **Add**.
11. In the Create a Resource Pool Wizard – Member Selection window that opens click Search.
12. Under **Available items** click **LON-MS2.CONTOSO.COM** and then click **Add** and then click **OK**.
13. Click **Next** on the **Pool Membership** page.
14. On the **Summary** page click **Create** and then on the **Completion** page click **Close**.
15. Click to open the **Synchronization Account** drop-down list, click **Alert Attachment Account**, and then click **Next**.
16. On the **Project Settings** page, click to open the **Project** drop-down list, and then click **Contoso Team Project**.
17. Click to open the **Area Path** drop-down list, click **Contoso Team Project**, and then click **Next**.
18. On the **Complete** page, click **Create**.

19. In the **Import Operations Issue Work Item Type Definition** window that opens, in the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
20. If a TFS Work Item Synchronization window opens, click Save.
21. Logon to LON-AP1 and create a folder in **C** name **TFS**.
22. Browse to **\LON-DC1\Media\SCOM2012R2\SupportTools\AMD64**.
23. Copy the **OperationalIssue\_11.xml** file to the **C:\TFS** folder on LON-AP1.
24. Open a command prompt and navigate to the **C:\TFS** folder.
25. Type the following command and then press enter:

```
"C:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\witadmin.exe"
importwitd /collection:http://lon-ap1:8080/tfs /p:"Contoso Team Project"
/f:OperationalIssue_11.xml"
```

26. Wait until the message stating **The work item type import has completed** appears and then close the command prompt window.

#### ► Task 3: Confirm TFS integration is working as expected

1. On LON-MS1, in the Operations console, click the **Monitoring** pane, and then expand **Application Monitoring**.
2. Expand **.NET Monitoring**, and then click **Active Alerts**.
3. In the details pane, right-click a **Server Performance Exception** alert, click **Set Resolution State**, and then click **Assigned to Engineering**.
4. Click the **Task Status** view, right-click inside the details pane, and then click **Refresh**.
5. Intermittently refresh the view until a new task named **TFS Create Work Item Task** is displayed. This can take up to 10 minutes.
6. Refresh the view until the **TFS Create Work Items Task** completes with a Status of **Success**.
7. Log on to LON-AP1, click **Start**, and then click **Visual Studio 2013**.
8. If a **Microsoft Visual Studio** window opens, click **No**.
9. In the **Microsoft Visual Studio (Administrator)** window that opens, click **Work Items**.
10. Under **Queries**, right-click **My Queries**, and then click **New Query**.
11. In the **New Query** window that opens, click **Run**.
12. In the **Query Results** window, double-click the **Work Item**.

 **Note:** You may need to expand the center pane to see the work item by dragging the two horizontal lines upwards.

13. In the **Operational Issue** window that opens, review the **Properties** and **Product Knowledge** sections to confirm the **Work Item** references the alert has been synchronized.
14. Close the **Work Item** and **Visual Studio 2013** windows.

**Results:** After this exercise, you should have installed and configured the TFS Work Item Synchronization Management Pack. You should have also configured the TFS Work Item Synchronization Management

Pack Template. Finally you should have confirmed TFS integration is working by assigning an alert to engineering in the Operations console, and then confirming a work item was created in TFS.



# Module 6: End to End Service Monitoring

## Lab: Configuring End-to-End Service Monitoring

### Exercise 1: Configure Agent Locations for the Summary Dashboard

#### ► Task 1: Create the locations

1. Log on to LON-MS1, click **Start**, type **Operations** and then click **Operations Manager Shell**.
2. In the **Administrator: Operations Manager Shell** window that opens, type the following commands pressing Enter after each command.

```
New-SCOMLocation -DisplayName "Redmond" -Latitude 47.6739882 -Longitude -122.121512
New-SCOMLocation -DisplayName "Chicago" -Latitude 41.850033 -Longitude -87.6500523
```

#### ► Task 2: Create location variables

1. Log on to LON-MS1, click **Start**, type **Operations** and then click **Operations Manager Shell**.
2. In the **Administrator: Operations Manager Shell** window that opens, type the following commands, pressing Enter after each command.

```
$redmond = Get-SCOMLocation -DisplayName "Redmond"
$chicago = Get-SCOMLocation -DisplayName "Chicago"
```

#### ► Task 3: Create the agent to location associations

1. Log on to **LON-MS1** and then click **Start**, type **Operations** and then click **Operations Manager Shell**.
2. In the **Administrator: Operations Manager Shell** window that opens, type the following commands pressing Enter after each command.

```
$Agent = Get-SCOMAgent -Name "LON-SQ1.contoso.com"
set-SCOMLocation -Location $Redmond -Agent $Agent
$Agent = Get-SCOMAgent -Name "LON-DC1.contoso.com"
set-SCOMLocation -Location $Chicago -Agent $Agent
```

**Results:** After this exercise, you should have used the Operations Manager shell to create new locations for Redmond and Chicago. You should have also associated these locations with the Operations Manager agents running on LON-SQ1 and LON-DC1.

## Exercise 2: Configure Synthetic Transactions

### ► Task 1: Create a Web Application Availability Monitor

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Authoring** pane, and then expand **Management Pack Templates**.
3. Click **Web Application Availability Monitoring**, and then in the **Tasks** pane, click **Add Monitoring Wizard**.
4. In the Add Monitoring Wizard, on the **Monitoring Type** page, click **Web Application Availability Monitoring**, and then click **Next**.
5. On the **General** page, in the **Name** box, type **DinnerNow Web Site Availability**, and then in the **Management pack** drop-down list, click **DinnerNow**.
6. On the **General** page, click **Next**.
7. On the **What to Monitor** page, in the **Name** box for the first URL, type **DinnerNow Home Page**.
8. In the **URL** box, type **http://LON-AP2/DinnerNow**.
9. Click **Next**.
10. On the **Where to Monitor From** page, click **Add**, and then in the **Select internal locations** window that opens, click **Search**.
11. Under Where to monitor, click LON-DC1.CONTOSO.COM and **LON-SQ1.CONTOSO.COM**, click Add, and then click OK.
12. On the **Where to Monitor From** page, click **Next**.
13. On the **View and Validate Tests** page, click **Run Test**.
14. In the **Test Results** window that opens, in the **Summary**, **Details**, **HTTP Request**, **HTTP Response** and **Raw Data** tabs, view the test result details.
15. In the **Test Results** window, click **Close**.
16. On the **View and Validate Tests** page, click **Next**.
17. On the **Summary** page, click **Create**.
18. Click the **Monitoring** pane, expand **Application Monitoring**, expand **Web Application Availability Monitoring**, and then click **Test State**.
19. Wait until the **DinnerNow Web Site Availability** tests appear and are in a healthy state.

### ► Task 2: View the DinnerNow web application availability by using the Summary and Detailed Dashboards

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Monitoring** pane, and then expand **Application Monitoring**.
3. Expand **Web Application Availability Monitoring**, and then click **Test State**.
4. In the details pane, click one of the tests.
5. In the **Tasks** pane, click **Summary Dashboard – Map**.
6. In the **Summary Dashboard Map – SCOM 2012 – Operations Manager** window that opens, notice that the health state for tests being run in Chicago and Redmond are displayed on the map.
7. Click each test location, and then view the **Test Status** information for each.

8. From the **Tasks** pane in the Operations console, click **Detailed Dashboard - List**.
9. In the **Detailed Dashboard - List – SCOM2012 – Operations Manager** window that opens, click **Chicago**, and then in the **Test Status** window, select the test.
10. Review the six performance counters for the selected test.
11. Select **Redmond**, and then in the **Test Status** window, select the test.
12. Review the six performance counters for the selected test.



**Note:** Performance counter data will not initially be displayed. This is normal. As data is collected from the web application availability monitor it will be displayed here later.

13. Close the **Detailed Dashboard – List – SCOM2012 – Operations Manager** window.
14. Close the **Summary Dashboard Map – SCOM 2012 – Operations Manager** window.

#### ► Task 3: Configure remote connections to LON-AP2

1. Logon to LON-AP2, click Start, All Programs, Microsoft SQL Server 2008, Configuration Tools and then click SQL Server Configuration Manager.
2. In the SQL Server Configuration Manager window that opens expand SQL Server Network Configuration and then click Protocols for SQLEXPRESS.
3. From the details pane right-click **TCP/IP** and then click **Enable**.
4. In the **Warning** window that opens click **OK**.
5. Close SQL Server Configuration Manager.
6. Open Windows Services and restart the SQL Server (SQLEXPRESS) service.
7. Log off LON-AP2.
8. Logon to LON-SC1 and then click **Start** then type **SQL Server** and then click **SQL Server Management Studio**.
9. In the **Connect to Server** window that opens type **LON-AP2\SQLEXPRESS** in the **Server name** box replacing any existing text and then click **Connect**.
10. In the **Object Explorer** pane expand **Security** and then click **Logins**.
11. Right-click **Logins** and then click **New Login**.
12. In the **Login – New** window that opens click **Search**.
13. In the **Select User or Group** window that opens click **Locations**, click **Entire Directory** and then click **OK**.
14. Type **svc\_SCOM2012\_msaa** in the Enter the object names to select box and then click Check Names and then click **OK**.
15. In the **Login – New** window click the **Server Roles** tab.
16. Under **Server roles** select **sysadmin** and then click **OK**.
17. Close **SQL Server Management Studio** and then log off LON-SC1.

#### ► Task 4: Create an OLE DB Data Source Monitor

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Authoring** pane, and then expand **Management Pack Templates**.

3. In the **Tasks** pane, click **Add Monitoring** Wizard.
4. In the Add Monitoring Wizard that opens, on the **Monitoring Type** page, click **OLE DB Data Source**, and then click **Next**.
5. On the **General Properties** page, in the **Name** box, type **DinnerNow Database Check**.
6. Click the **Management Pack** drop-down list, click **DinnerNow**, and then click **Next**.
7. On the **Connection String** page, click **Build**.
8. In the **Build Connection String** window that opens, click the **Provider** drop-down list, and then click **Microsoft OLE DB Provider for SQL Server**.
9. In the **Computer or device name** box, type **LON-AP2\SQLEXPRESS**
10. In the **Database** box, type **DinnerNow**, and then click **OK**.
11. Select **Query to execute**, and then type the following in the box:

```
select * from dbo.menu
```

12. Click **Test**.
13. Notice the **Request processed successfully** message that appears, review the test results, and then click **Next**.
14. On the **Query Performance** page, click **Next**.
15. On the **Watcher Nodes** page, select **LON-MS1** and then click **Next**.
16. On the **Summary** page, click **Create**.
17. Click the **Monitoring** pane, and then expand the **Synthetic Transaction** folder.
18. Click **OLE DB Data Source State** and, in the details pane, wait until the **DinnerNow Database Check** monitor is displayed in a healthy state.



**Note:** It can take up to 5 minutes for the DinnerNow Database Check monitor to appear.

## ► Task 5: Create a TCP Port Check Monitor

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Authoring** pane, and then expand **Management Pack Templates**.
3. In the **Tasks** pane, click **Add Monitoring** Wizard.
4. In the Add Monitoring Wizard that opens, on the **Monitoring Type** page, click **TCP Port**, and then click **Next**.
5. On the **General Properties** page, in the **Name** box, type **DinnerNow Web Site Port Check**.
6. In the **Management Pack** drop-down list, click **DinnerNow**, and then click **Next**.
7. On the **Target and Port** page, in the **Computer or device name** box, type **LON-AP2**.
8. In the **Port** box, type **80**, and then click **Test**.
9. Notice the **Request processed successfully** message that appears, review the request information, and then click **Next**.
10. On the **Watcher Node** page, select **LON-SQ1.CONTOSO.COM** and **LON-MS1.CONTOSO.COM**, and then click **Next**.

11. On the **Summary** page, click **Create**.
12. Click the **Monitoring** pane, and then expand the **Synthetic Transaction** folder.
13. Click **TCP Port Checks State**, and then in the details pane, wait until the **DinnerNow Database Check** monitor is displayed in a healthy state.

**Results:** After this exercise, you should have used the Operations Manager Management Pack templates to create a Web Application Availability Monitor, an OLE DB Data Source Monitor and a TCP Port Check Monitor for the DinnerNow .NET web application.

## Exercise 3: Create a Distributed Application Diagram for Dinner Now

### ► Task 1: Create the Distributed Application Diagram

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Authoring** pane, and then click **Distributed Applications**.
3. In the **Tasks** pane, click **Create a New Distributed Application**.
4. In the **Distributed Application Designer** window that opens, in the **Name** box, type **DinnerNow**.
5. Under **Template**, click **Line of Business Web Application**.
6. Click the **Management Pack** drop-down list, click **DinnerNow**, and then click **OK**.
7. In the **Distributed Application Designer** window, click **OK**.
8. In the **Distributed Application Designer – DinnerNow** window that opens, click the **Database** pane.
9. Under **Object**, right-click the **DinnerNow** database, click **Add To**, and then click **DinnerNow Web Application Databases**.
10. Click the **Web Site** pane, and under **Object**, right-click the default website for LON-AP2.
11. Click **Add To**, and then click **DinnerNow Web Application Web Sites**.

### ► Task 2: Add the Windows Server 2008 Operating System component group

1. From the toolbar, click **Add Component**.
2. In the **Create New Component Group** window that opens, in the **Name your component group** box, type **Windows Server 2008 Operating System**.
3. Select **Objects of the following type(s)**, browse to **Object\Configuration Item\Logical Entity\Operating System\Windows Operating System\Windows Server Operating System**, and then select **Windows Server 2008 Operating System**.
4. In the **Create New Component Group** window, click **OK**.
5. Under **Windows Server 2008 Operating System**, right-click **LON-AP2.contoso.com**, click **Add To**, and then click **Windows Server 2008 Operating System**.

### ► Task 3: Add the IIS Server Role component group

1. On the toolbar, click **Add Component**.
2. In the **Create New Component Group** window that opens, in the **Name your component group** box, type **IIS Server Role**.
3. Select **Objects of the following type(s)**, browse to **Object\Configuration Item\Logical Entity\Computer Role\Windows Computer Role**, and then select **IIS Server Role**.
4. In the **Create New Component Group** window, click **OK**.
5. Under **IIS Server Role**, right-click **LON-AP2.contoso.com**, click **Add To**, and then click **IIS Server Role**.

### ► Task 4: Add the SQL Server Role component group

1. On the toolbar, click **Add Component**.
2. In the **Create New Component Group** window that opens, in the **Name your component group** box, type **SQL Server Role**.

3. Select **Objects of the following type(s)**, browse to **Object\Configuration Item\Logical Entity\Computer Role\Windows Computer Role**, and then select **SQL Role**.
4. In the **Create New Component Group** window, click **OK**.
5. Under **SQL Role**, right-click **LON-AP2.contoso.com**, click **Add To**, and then click **SQL Server Role**.

► **Task 5: Add the Web Application Availability component group**

1. On the toolbar, click **Add Component**.
2. In the **Create New Component Group** window that opens, in the **Name your component group** box, type **Web Application Availability**.
3. Select **Objects of the following type(s)**, browse to **Object\Configuration Item\Logical Entity\Perspective**, and then select **Web Application Availability Monitoring Test Base**.
4. In the **Create New Component Group** window, click **OK**.
5. In the Replace Visible Object Type window that opens, click Replace the selected visible Object Type button with the new one, click the drop-down list and then click Distributed Application Component and then click OK.
6. Under **Web Application Availability Monitoring Test Base**, right-click each object, click **Add To**, and then click **Web Application Availability**.

► **Task 6: Add the DinnerNow Database Availability component group**

1. From the toolbar, click **Add Component**.
2. In the **Create New Component Group** window that opens, type **DinnerNow Database Availability** in the **Name your component group** text box.
3. Select **Objects of the following type(s)**, browse to **Object\Configuration Item\Logical Entity\Perspective** and then select **OLE DB Check Perspective**.
4. Click **OK** on the **Create New Component Group** window.
5. In the Replace Visible Object Type window that opens, click Replace the selected visible Object Type button with the new one, click the drop-down list and then click Web Application Availability Monitoring Test Base (2) and then click OK.
6. Under **OLE DB check Perspective** right-click **DinnerNow Database Check** and then click **Add To** and then click **DinnerNow Database Availability**

► **Task 7: Add the TCP Port Check Component Group**

1. On the toolbar, click **Add Component**.
2. In the **Create New Component Group** window that opens, in the **Name your component group** box, type **TCP Port Availability**.
3. Select **Objects of the following type(s)**, browse to **Object\Configuration Item\Logical Entity\Perspective**, and then select **TCP Port check Perspective**.
4. In the **Create New Component Group** window, click **OK**.
5. In the Replace Visible Object Type window that opens, click Replace the selected visible Object Type button with the new one, click the drop-down list and then click OLE DB Check Perspective and then click OK.
6. Under **TCP port check Perspective**, right-click each object, click **Add To**, and then click **TCP Port Availability**.

► **Task 8: Create the relationships between component groups**

1. From the toolbar, click **Create Relationship**.
2. Drag DinnerNow Web Application Web Sites to IIS Server Role.
3. Drag IIS Server Role to Windows Server 2008 Operating System.
4. Drag SQL Server Role to Windows Server 2008 Operating System.
5. Drag DinnerNow Web Application Databases to SQL Server Role.
6. Drag Web Application Availability to DinnerNow Web Application Web Sites.
7. Drag DinnerNow Database Availability to DinnerNow Web Application Databases.
8. Drag TCP Port Availability to DinnerNow Web Application Web Sites.
9. On the toolbar, click **Save**.
10. Close the **Distributed Application Designer – DinnerNow** window.

► **Task 9: View the Distributed Application Diagram**

1. Click the Monitoring pane, and then click Distributed Applications.
2. In the details pane, click **DinnerNow**, and then in the **Tasks** pane, click **Diagram View**.
3. In the **Operations Manager** window that opens, click **Yes**.
4. View the **DinnerNow** Distributed Application Diagram.

**Results:**

After this exercise, you should have created a Distributed Application Diagram for the DinnerNow web application. The Distributed Application Diagram includes the Database, Web Site, Operating System, IIS Server Role, and SQL Server Role components. After completing the Distributed Application Diagram, you use the Diagram View from the Monitoring pane to view the health of the DinnerNow web application.

## Exercise 4: Create a Visio diagram of the distributed application

### ► Task 1: Configure the Visio add-in

1. Log on to LON-AP2, and on the desktop, double-click **Microsoft Visio 2010**.
2. If a Microsoft Office Activation Wizard opens, click Close.
3. In the Microsoft Visio window that opens, click **New**; under **Other Ways to Get Started**, click **Blank drawing**, and then click **Create**.
4. On the ribbon, click the **Operations Manager** tab, and then click **Configure**.
5. In the **Configure Data Source** window that opens, in the **Name** box, type **LON-MS1**.
6. In the **Address** box, type **http://LON-MS1/OperationsManager**.
7. Select **Automatically refresh data**, and then click **OK**.
8. Leave Visio open.

### ► Task 2: Export the DinnerNow Distributed Application Diagram

1. Log on to LON-MS1, and open the Operations console.
2. Click the **Monitoring** pane, and then click **Distributed Applications**.
3. In the details pane, click **DinnerNow**, and then in the **Tasks** pane, click **Diagram View**.
4. In the **Operations Manager** pop-up window, click **Yes**.
5. After the **Diagram View - SCOM2012 - Operations Manager** opens, from the toolbar, click the **Export Page to Visio** button.
6. In the **Export Page to Visio VDX** window that opens, in the **File name** box, type **\\\lon-ap2\c\$**, and then press Enter.
7. In the **File name** box, type **DinnerNow.vdx**, and then click **Save**.
8. Leave the **Diagram View - SCOM2012 - Operations Manager** window open.

### ► Task 3: Import the DinnerNow Distributed Application Diagram into Visio

1. On LON-AP2, in Visio, click the **File** menu, and then click **Open**.
2. Browse to Drive C, click **DinnerNow**, and then click **Open**.
3. Notice the Distributed Application Diagram has loaded and shows the current health state.
4. On the **Operations Manager** tab, click **Configure**.
5. Ensure the **Automatically refresh data** option is selected, and then click **OK**.
6. Leave Visio open.

### ► Task 4: Simulate a failure in DinnerNow and view the health state in the Visio diagram

1. On LON-AP2, click **Start**, click **Administrative Tools**, and then click **Services**.
2. In the **Services** window that opens, right-click **World Wide Web Publishing Service**, and then click **Stop**.
3. On LON-MS1, right-click inside the **Diagram View - SCOM2012 - Operations Manager**, and then click **Refresh**.
4. In the **Operations Manager** window that opens click **Yes**.

5. Notice the **DinnerNow Web Application** component group is now in an unhealthy state.
6. On LON-AP2, in the Visio diagram, click the **Operation Manager** tab, and then click **Refresh**.
7. Notice **DinnerNow Web Application** is now shown in a critical state.
8. On LON-AP2, in **Services**, right-click the **World Wide Web Publishing Service**, and then click **Start**.
9. On LON-MS1, right-click inside the **Diagram View - SCOM2012 - Operations Manager**, and then click **Refresh**.
10. In the **Operations Manager** window that opens click **Yes**.
11. Notice the **DinnerNow Web Application** component group is now in a healthy state.
12. On LON-AP2, In Visio, on the **Operations Manager** tab, click **Refresh**.
13. Notice **DinnerNow Web Application** is now shown in a healthy state.
14. Save the Visio diagram, and then close Visio.

**Results:** After this exercise, you should have created a Visio diagram of the DinnerNow Distributed Application Diagram and confirmed that the health state is updated correctly in Visio.

# Module 7: Scorecards, Dashboards, and Reporting

## Lab: Configuring Reporting, Dashboards, and Service Level Tracking

### Exercise 1: Design a New Report

#### ► Task 1: Import the report model into the Report Server

1. Log on to LON-MS1 and start Microsoft Internet Explorer.
2. In Internet Explorer, browse to **HTTP://LON-SQ1/Reports**.
3. On the **SQL Server Reporting Services** webpage, on the right side of the page under **Search**, click **Details View**.
4. Click **Upload File**.
5. On the **Upload File** webpage, click **Browse**.
6. In the **Choose File to Upload** dialog box, in the **File name** box, type **\LON-DC1\Media\SCOM2012R2\ReportModels\Other**, and then press Enter.
7. Click **Event.smdl**, and then click **Open**.
8. On the **Upload File** webpage, click **OK**.
9. On the **SQL Server Reporting Services** webpage, under the **Name** column, click **Event**.
10. On the **Event** webpage, click the **Data Sources** tab, and then click **Browse**.
11. Under the **Location** box, expand **Home**, click **Data Warehouse Main**, click **OK**, and then click **Apply**.
12. In the upper-right corner of the webpage, click **Home**.
13. Close Internet Explorer.

#### ► Task 2: Design a new report using Report Builder

1. On LON-MS1, open Internet Explorer, and then browse to **http://LON-SQ1/reportserver/reportbuilder/reportbuilder\_3\_0\_0\_0.application**.
2. In the **Application Run – Security Warning** pop-up dialog box, click **Run**.  
Report Builder 3.0 opens.
3. On the **Getting Started** page of the **Report Builder**, on the **New Report** tab, click **Chart Wizard**.
4. On the **Choose a dataset** page, click **Next**.
5. On the **Choose a connection to a data source** page, click **Browse**.
6. In the **Select Data Source** window that opens, click **Event**, and then click **Open**.
7. On the **Choose a connection to a data source** page, make sure that **Event** is selected, and then click **Next**.
8. On the **Design a query** page, under **Entities**, click **Event**.
9. Under **Fields**, drag **Event Logging Computer Name** to the **Drag and drop column fields** box, which is in the pane at the right.
10. Under **Fields**, drag **#Events** to the right side of **Event Logging Computer**, in the pane to the right.
11. On the toolbar, click **Filter**.

12. In the **Filter Data** window that opens, under **Fields**, drag **Event Display Number** to the pane on the right, under **Events with**.
13. Click the **(no values selected)** link, and then in the **Filter List** window that opens, under **Available data**, double-click **6005** to add the event ID into the **Selected data** window, and then click **OK**.
14. In the **Filter Data** window, click **OK**.
15. On the **Design a query** page, click **Next**.
16. On the **Choose a chart type** page, click **Column**, and then click **Next**.
17. On the **Arrange chart fields** page, drag the **Event\_logging\_Computer\_Name** field to the **Categories** section, drag the **ID\_Events** field to the **Values** section, and then click **Next**.
18. On the **Choose a style** page, click **Finish**.
19. In the **Untitled – Microsoft SQL Server Report Builder** window, in the pane to the right, edit the **Chart Title** name to **Number of computer restarts within the last 7 days**.
20. Expand the chart by using the placeholders so that the chart includes the whole page.
21. Click the x **Axis Title**, and rename it **Computer**.
22. Click the y **Axis title**, and rename it **No. of restarts**.
23. Right-click the **ID Events** legend, and then click **Delete Legend**.
24. On the toolbar, click **Save As**; in the **Save As Report** window that opens, double-click the **Microsoft.Windows.Server.2012.Monitoring** folder; in the **Name box**, type **Number of computer restarts within the last 7 days.rdl**; and then click **Save**.
25. Close the **Number of computer restarts within the last 7 days – Microsoft SQL Server Report Builder** window.

#### ► Task 3: View the report

1. On LON-MS1, in the Operations console, click the **Reporting** pane.
2. Expand **Reporting**, and then click **Windows Server 2012 Operating System (Monitoring)**.
3. In the **Details** pane, click **Number of computer restarts within the last 7 days**, and then in the **Tasks** pane, click **Open**.
4. Review the report that opens, and then close the report window.

**Results:** After this exercise, you should have used Report Builder to design a new report that shows how many times in the last seven days the computers have restarted. Also, you should have saved the report to the SSRS so that the report is available from the Reporting pane of the Operations console.

## Exercise 2: Schedule Reports

### ► Task 1: Create a file share and schedule the report

1. On LON-MS1, create a folder on drive C that is named **Reports**, and then share the folder so that everyone has the read/write permission level.
2. Open the Operations console.
3. Click the **Reporting** pane, expand **Reporting**, and then click **Windows Server 2012 Operating System (Monitoring)**.
4. In the **Details** pane, click **Number of computer restarts within the last 7 days**, and then in the **Tasks** pane, click **Open**.
5. Confirm that the report opens successfully, and then on the **File** menu, click **Schedule**.
6. In the **Subscribe To A Report – Number Of Computer Restarts Within The Last 7 Days** wizard, on the **Delivery Settings** page, in the **Description** box, type **Number of computer restarts within the last 7 days**.
7. Under **Delivery method**, click the drop-down menu, and then select **Windows File Share**.
8. In the **File name (required)** box, type **Number of computer restarts within the last 7 days.mhtml**.
9. In the **Path (required)** box, type **\\\LON-MS1\Reports**.
10. Click the **Render Format (required)** drop-down menu, and then click **MHTML (Web Archive)**.
11. Click the **Write mode** drop-down menu, and then click **Autoincrement**.
12. In the **User name (required)** box, type **Contoso\Administrator**.
13. In the **Password (required)** box, type **Pa\$\$w0rd**, and then click **Next**.
14. On the **Subscription Schedule** page, select **Weekly**; in the **The subscription is effective beginning** box, increase the current time by two minutes; and then click **Next**.
15. On the **Parameters** page, click **Finish**.
16. Close the report window.

### ► Task 2: Confirm the report schedule is working as expected

1. On LON-MS1, open the **C:\Reports** folder.
2. Wait until the time specified in step 14 of Exercise 2, Task 1 has passed.
3. Refresh the contents of the folder, and then confirm the **Number of computer restarts within the last 7 days.mhtml** file is displayed.
4. Double-click **Number of computer restarts within the last 7 days.mhtml**, and then review the report.
5. Close the report window.

**Results:** After this exercise, you should have scheduled the Number Of Computer Restarts Within The Last 7 Days report to run weekly, and then exported this report as an MHTML file to the Reports share site on LON-MS1. You should also have confirmed that the schedule works as expected and that the report is generated.

## Exercise 3: Configure Service Level Tracking for DinnerNow

### ► Task 1: Create a service level objective

1. On LON-MS1, open the Operations console.
2. Click the **Authoring** pane, and expand **Management Pack Objects** and then click **Service Level Tracking**.
3. From the **Tasks** pane, click **Create**.
4. In the Service Level Tracking wizard, on the **General** page, in the **Name** box, type **DinnerNow**, and then click **Next**.
5. On the **Objects to Track** page, click **Select**; in the **Select a Target Class** dialog box that opens, in the **Look for** box, type **IIS 7**; and then in the **Search result filter** drop-down list, click **All**.
6. From the list of classes, click **IIS 7 Web Server**, and then click **OK**.
7. Under **Scope**, select **A group or object that contains objects of the targeted class**, and then click **Select**.
8. In the **Select an Object** dialog box that opens, in the **Look for** box, type **AP2**, and then click **Search**.
9. From the list of objects, click **LON-AP2.CONTOSO.COM**, where the **Class** column displays **Windows Server 2008 R2 Full Computer**, and then click **OK**.
10. Click the drop-down list next to **Management Pack**, and then click **DinnerNow**.
11. On the **Objects to Track** page, click **Next**.
12. On the **Service Level Objectives** page, click **Add**, and then click **Monitor state SLO**.
13. In the **Service Level Objective (Monitor State)** window that opens, in the **Service level objective name** box, type **Availability**, and then click **OK**.
14. On the **Service Level Objectives** page, note the default service level objective value, and then click **Next**.
15. On the **Summary** page, click **Finish**.
16. On the **Completion** page, click **Close**.

### ► Task 2: View the Service Level Tracking Summary Report

1. On LON-MS1, open the Operations console.
2. Click the **Reporting** pane, expand **Reporting**, and then click **Microsoft Service Level Report Library**.
3. In the **Details** pane, click **Service Level Tracking Summary Report**.
4. In the **Tasks** pane, click **Open**.
5. In the **Service Level Tracking Summary Report – Operations Manager – Report – SCOM2012** window that opens, click **Add**.
6. In the **Add Service Levels** window that opens, click **Search**.
7. Under available items, click **DinnerNow**, click **Add**, and then click **OK**.
8. Click the **From** drop-down list, and then click **Yesterday**.
9. Click **Run** to run the report.
10. In **Service Level Tracking Summary Report**, expand **SCOM2012 | LON-AP2.CONTOSO.COM**, and then click **Availability** to view the report details.

- 
11. Close the report window.

**Results:** After this exercise, you should have configured a Service Level Object that is targeted at the DinnerNow Web Server. You should have also run the Service Level Tracking Summary Report and included the DinnerNow service level tracking objective.

## Exercise 4: Configure an Alert Dashboard

### ► Task 1: Create the dashboard

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Monitoring** pane, right-click the **DinnerNow** folder, click **New**, and then click **Dashboard View**.
3. In the New Dashboard and Widget Wizard that starts, on the **Template** page, click **Column Layout**, and then click **Next**.
4. On the **General Properties** page, in the **Name** box, type **DinnerNow Critical and Warning Alerts**, and then click **Next**.
5. On the **Column Count** page, increase the number of columns to **2**, and then click **Next**.
6. On the **Summary** page, click **Create**.
7. On the **Completion** page, click **Close**.

### ► Task 2: Configure the widgets

1. In the DinnerNow Critical and Warning Alerts dashboard, click the Click to add widget link at the left.
2. In the New Dashboards and Widget Wizard that starts, on the **Template** page, click **Alert Widget**, and then click **Next**.
3. On the General Properties page, in the **Name** box, type Critical and Warning Alerts, and then click **Next**.
4. On the **Scope** page, click the **ellipsis** button (...).
5. In the **Select a group or object** dialog box that opens, select **Groups and objects**; in the **Enter Text to search for a match with names of objects or groups** box, type **dinnernow**; and then click the **magnifying glass**.
6. From the list of **Available items**, click **DinnerNow - Production**, where .NET Application Component Group is displayed in the Class column and then click **OK**.
7. On the **Scope** page, click **Next**.
8. On the **Criteria** page, select **Critical** and **Warning**, and then click **Next**.
9. On the **Specify Display Preferences** page, click **Next**.
10. On the **Summary** page, click **Create**.
11. On the **Completion** page, click **Close**.
12. In the **DinnerNow Critical and Warning Alerts** dashboard, click the Click to add widget link to the right.
13. In the New Dashboard and Widget Wizard, on the **Template** page, click **Details Widget**, and then click **Next**.
14. On the **General Properties** page, in the **Name** box, type **Alert Details**, and then click **Next**.
15. On the **Summary** page, click **Create**.
16. On the **Completion** page, click **Close**.

### ► Task 3: Use the Alert Dashboard

1. In the **DinnerNow Critical and Warning Alerts** dashboard, select an alert in the **Critical and Warning Alerts** column.

- 
2. In the **Alert Details** column, notice that the alert details for the selected alert are displayed.

**Results:** After this exercise, you should have created a dashboard view that uses the alert and details widgets to display critical and warning alerts for the DinnerNow .NET Framework application.

## Exercise 5: Configure a Performance Dashboard

### ► Task 1: Create the dashboard

1. Click the **Monitoring** pane, right-click the **DinnerNow** folder, click **New**, and then click **Dashboard View**.
2. In the New Dashboard and Widget Wizard that starts, on the **Template** page, click **Grid Layout**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **DinnerNow – End User Performance**, and then click **Next**.
4. On the **Layout** page, select **2 Cells**, click **second cell type**, and then click **Next**.
5. On the **Summary** page, click **Create**.
6. On the **Completion** page, click **Close**.

### ► Task 2: Configure the widgets

1. In the **DinnerNow – End User Performance** dashboard, click the first **Click to add widget** link.
2. In the New Dashboards and Widget Wizard, on the **Template** page, click **Performance Widget**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **Average Request Time (seconds)**, and then click **Next**.
4. On the **Scope and Counters** page, click the (...) button.
5. In the **Select a group or object** window that opens, select **Groups and objects**; in the **Enter text to search for a match with names of objects or groups** box, type **dinnernow**; and then click the magnifying glass icon.
6. From the list of **Available items**, click **Default Web Site/DinnerNow**, where **ASP.NET Application** is displayed in the **Class** column and then click **OK**.
7. Click **Add**.
8. In the **Select performance counters** window that opens, click the **Object** drop-down list, and then click **.NET Apps**.
9. Click the **Counter** drop-down list, and then click **Avg. Request Time (seconds)**.
10. Under **Available items**, click **.NET Apps**, where the **Performance Instance** column does not display **(All)**, click **Add**, and then click **OK**.
11. On the **Scope and Counters** page, click **Next**.
12. On the **Time Range** page, click **Next**.
13. On the **Chart Preferences** page, click **Next**.
14. On the **Summary** page, click **Create**.
15. On the **Completion** page, click **Close**.
16. In the **DinnerNow – End User Performance** dashboard, click the second **Click to add widget** link.
17. In the New Dashboards and Widget Wizard, on the **Template** page, click **Performance Widget**, and then click **Next**.
18. On the **General Properties** page, in the **Name** box, type **Exception Events (per second)**, and then click **Next**.

19. On the **Scope and Counters** page, click the (...) button.
20. In the **Select a group or object** window that opens, select **Groups and objects**; in the **Enter text to search for a match with names of objects or groups** box, type **dinnernow**; and then click the magnifying glass.
21. From the list of **Available items**, click **Default Web Site/DinnerNow**, where **ASP.NET Application** is displayed in the **Class** column and then click **OK**.
22. Click **Add**.
23. In the **Select performance counters** window that opens, click the **Object** drop-down list, and then click **.NET Apps**.
24. Click the **Counter** drop-down list, and then click **Exception Events/sec**.
25. Under **Available items**, click **.NET Apps**, where the **Performance Instance** column does not display **(All)**, click **Add**, and then click **OK**.
26. On the **Scope and Counters** page, click **Next**.
27. On the **Time Range** page, click **Next**.
28. On the **Chart Preferences** page, click **Next**.
29. On the **Summary** page, click **Create**.
30. On the **Completion** page, click **Close**.

**Results:** After this exercise, you should have created a new dashboard view that uses the performance widget. You should have added the Transaction Response Time and Total Monitored Requests/Sec performance counters that the widgets display in the dashboard.

## Exercise 6: Configure a Summary Dashboard

### ► Task 1: Create the dashboard

1. Click the **Monitoring** pane, right-click the **DinnerNow** folder, click **New**, and then click **Dashboard View**.
2. In the New Dashboard and Widget Wizard that starts, on the **Template** page, click **Summary Dashboard**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **DinnerNow**, and then click **Next**.
4. On the **Summary** page, click **Create**.
5. On the **Completion** page, click **Close**.

### ► Task 2: Configure the widgets

1. In the **DinnerNow** dashboard next to the **Top N** section, click the configuration icon, and then click **Configure**.
2. In the Update Configuration wizard, on the **General Properties** page, in the **Name** box, type **Database Free Space (MB)**, and then click **Next**.
3. On the **Scope and Counters** page, next to **Select a group or object**, click the (...) button.
4. In the **Select a group or object** window, select **Groups and objects**; in the **Enter text to search for a match with names of objects or groups** box, type **DinnerNow**; and then click the **magnifying glass**.
5. Click **DinnerNow**, where the **Class** column displays **SQL Database**, and then click **OK**.
6. Next to **Select a performance counter (Object/Counter/Instance)**, click the (...) button.
7. In the **Select a performance counter (Object/ Counter/ Instance)** window, under **Object**, select **MSSQL\$SQLEXPRESS:Database**.
8. Under **Counter**, select **DB Total Free Space (MB)**.
9. Under **Instance**, select **DinnerNow**.
10. In the **Available items** list, click **DinnerNow** and then click **OK**.
11. On the **Scope and Counters** page, click **Next**.
12. On the **Time Range and Results** page, click **Next**.
13. On the **Display** page, click **Finish**.
14. Next to the **Performance** section, click the configuration icon, and then click **Configure**.
15. In the Update Configuration wizard, on the **General Properties** page, in the **Name** box, type **Database Free Space (%)**, and then click **Next**.
16. On the **Scope and Counters** page, click the (...) button.
17. In the **Select a group or object** window, select **Groups and objects**; in the **Enter text to search for a match with names of objects or groups** box, type **DinnerNow**; and then click the **magnifying glass**.
18. Select the **DinnerNow** database, where the **Class** column displays **SQL Database**, and then click **OK**.
19. Under **Select performance counters**, click **Add**.
20. In the **Select performance counters** window, under **Object**, select **MSSQL\$SQLEXPRESS:Database**.
21. Under **Counter**, select **DB Total Free Space (%)**.

22. Under Instance, select DinnerNow.
23. Under **Available items**, click **DinnerNow**, click **Add**, and then click **OK**.
24. On the **Scope and Counters** page, click **Next**.
25. On the **Time Range** page, click **Next**.
26. On the **Chart Preferences** page, click **Finish**.
27. Next to the **State section**, click the configuration icon, and then click **Configure**.
28. In the Update Configuration wizard, on the **General Properties** page, in the **Name** box, type **SQL Server Health State**, and then click **Next**.
29. On the **Scope** page, click **Add**.
30. In the **Add Groups or Objects** window, select **Show all objects and groups**; in the **Enter text to search for a match with names of objects or groups** box, type **SQL**; and then click the **magnifying glass**.
31. In the **Available items** list, click **SQLEXPRESS**, where the **Path** displays **LON-AP2.CONTOSO.COM**; click **Add**; and then click **OK**.
32. On the **Scope** page, click **Next**.
33. On the **Criteria** page, click **Next**.
34. On the **Display** page, click **Finish**.
35. In the **Alerts** section, click the configuration icon, and then click **Configure**.
36. In the Update Configuration wizard, on the **General Properties** page, in the **Name** box, type **All SQL Server Alerts**, and then click **Next**.
37. On the **Scope** page, click the (...) button.
38. In the **Select a group or object** window, click the **Groups and objects** option, in the **Enter text to search for a match with names of objects or groups** box, type **SQL**; and then click the **magnifying glass**.
39. In the **Available items** list, click **SQLEXPRESS**, where the **Path** displays **LON-AP2.CONTOSO.COM**, and then click **OK**.
40. On the **Scope** page, click **Next**.
41. On the **Criteria** page, click **Next**.
42. On the **Specify Display Preferences** page, click **Finish**.



**Note:** If the **MSSQL\$SQLExpress:Database** performance counter is not available when configuring the widgets, perform the following steps and then restart this task from the beginning:

1. Cancel any open wizards in the Operations console.
2. Logon to **LON-AP2**.
3. Open **Internet Explorer** and browse to <http://lon-ap2/DinnerNow> and ensure the **Food Type** and **Meal** drop-down lists are populated. If they are not, close **Internet Explorer** and use the **DinnerNow SQL DB Detacher** from the desktop to re-attach the database,
4. Open **Internet Information Services (IIS) Manager**.

5. Expand **LON-AP2**, expand **Sites**, expand **Default Web Site** and then right-click **DinnerNow**.
6. Click **Manage Application** then click **Browse**.
7. Close **Internet Information Services (IIS) Manager** and the **Internet Explorer** windows.
8. Logoff **LON-AP2**.

**Results:** After this exercise, you should have created a Summary Dashboard view that contains the DinnerNow Database free space in MB and as a percentage. The view also shows the health state of computer running the SQL Server that DinnerNow relies on and any related alerts that are generated on the computer running SQL Server.

## Exercise 7: Configure the SLA Dashboard and publish the dashboard to SharePoint

### ► Task 1: Create the dashboard

1. Click the **Monitoring** pane, right-click the **DinnerNow** folder and then click **New**, and then click **Dashboard View**.
2. In the New Dashboard and Widget Wizard that starts, on the **Template** page, click **Service Level Dashboard**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **DinnerNow SLA**, and then click **Next**.
4. On the **Scope** page, click **Add**.
5. In the **Add SLA** window that opens, click **DinnerNow**, and click **Add**, and then click **OK**.
6. On the **Scope** page, click **Next**.
7. On the **Summary** page, click **Create**.
8. On the **Completion** page, click **Close**.

### ► Task 2: Publish the dashboard to SharePoint

1. Log on to LON-AP1 and open **Internet Explorer**.
2. In Internet Explorer, browse to <http://LON-AP1:8081/SitePages/Home.aspx>

 **Note:** As per the instructor note at the beginning of this lab, the SharePoint home page should already be loaded, if so, steps 1 and 2 above can be skipped.

3. On the **Microsoft SharePoint** home page, click the cog icon in the upper-right of the page and then click **Add a Page**.
4. In the **Add a page** dialog box that opens, in the **New page name** box, type **DinnerNow\_Availability**, and then click **Create**.

 **Note:** If a 401 Unauthorized page appears close Internet Explorer and then re-open it and browse to [http://lon-AP1:8081/SitePages/DinnerNow\\_Availability.aspx](http://lon-AP1:8081/SitePages/DinnerNow_Availability.aspx)

5. In the **DinnerNow\_Availability** web page that opens click **Page** and then click **Edit**.
6. Click the **Insert** tab and then click **Web Part**.
7. Under **Categories**, click **Microsoft System Center**, and then on the right side of the page, click **Add**.
8. Move the pointer to the right side of the page, click the drop-down menu that appears, and then click **Edit Web Part**.
9. Open a new **Internet Explorer** tab, and make sure that the original tab is left open.
10. In the new Internet Explorer tab, browse to <http://LON-MS1/OperationsManager>.
11. On the Web Console Configuration Required page click **Configure** and then click **Run**.
12. On the Web Console Configuration Tool window that opens click **Close**.
13. On the Web Console Configuration Required page click **Skip** and then click **Sign In**.

14. In the Operations Manager Web Console, from the Monitoring pane, expand DinnerNow, and then click DinnerNow SLA.
15. Wait for the page to load, and then copy the **URL** from the **Internet Explorer** address bar.
16. Go back to the original tab, and then paste the URL into the **Dashboard link** box.
17. Scroll down the page, and then click **OK**.
18. Click the **Save** icon on the toolbar and the wait until the **DinnerNow\_Availability** page is displayed with the **Operations Manager Dashboard Viewer Web Part**.
19. Log on to LON-MS1 and open **Internet Explorer**.
20. Browse to **http://LON-AP1:8081/SitePages/DinnerNow\_Availability.aspx**.

Notice that the new SharePoint page is displayed and includes the **Dinner Now SLA Dashboard**.



**Note:** You may need to refresh the web page for the DinnerNow SLA Dashboard to be displayed.

**Results:** After this exercise, you should have created an SLA Dashboard view that uses the DinnerNow website service level objectives that were previously created. You should then have created a new SharePoint page and added the SLA Dashboard view to the page so that the SLA Dashboard view is available to SharePoint users.

## Exercise 8: Use the GTM tool to publish a custom dashboard

### ► Task 1: Create a new Management Pack

1. Log on to LON-MS1 and open the Operations console.
2. Click the **Administration** pane, and then click **Management Packs**.
3. From the **Tasks** pane, click **Create Management Pack**.
4. In the **Create a Management Pack** wizard that starts, on the **General Properties** page, in the **Name** box, type **Windows Server Performance Dashboard**, and then click **Next**.
5. On the **Knowledge** page, click **Create**.

### ► Task 2: Create a new dashboard view

1. Click the **Monitoring** pane, right-click the **Windows Server Performance Dashboard** folder, click **New**, and then click **Dashboard View**.
2. In the New Dashboard and Widget Wizard that starts, on the **Template** page, click **Grid Layout**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **Windows Server Performance**, and then click **Next**.
4. On the **Layout** page, select **4-Cells**, select the second **Layout Template**, and then click **Next**.
5. On the **Summary** page, click **Create**.
6. On the **Completion** page, click **Close**.

### ► Task 3: Configure the first widget

1. In the **Windows Server Performance** view, click the upper-left **Click** to add widget link.
2. In the New Dashboard and Widget Wizard, on the **Template** page, select **Performance Widget**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **Memory Utilization**, and then click **Next**.
4. On the **Scope and Counters** page, click the (...) button, and then in the **Select a group or object** window that opens, in the **Filter** box, type **Windows Server**.
5. Under **Available items**, select **Windows Server Computer Group**, and then click **OK**.
6. On the **Scope and Counters** page, click **Add**.
7. In the **Select performance counters** window that opens, under **Object**, select **Memory**; and under **Counter**, select **PercentMemoryUsed**.
8. Under **Available items**, select **Memory**, where the **Performance Instance** column is blank, click **Add**, and then click **OK**.
9. On the **Scope and Counters** page, click **Next**.
10. On the **Time Range** page, in the **Last** box, type **5**, change **Hours** to **Days**, and then click **Next**.
11. On the **Chart Preferences** page, click **Next**.
12. On the **Summary** page, click **Create**.
13. On the **Completion** page, click **Close**.

### ► Task 4: Configure the second widget

1. In the **Windows Server Performance** view, click the upper-right **Click** to add widget link.

2. In the New Dashboard and Widget Wizard, on the **Template** page, select **Performance Widget**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **CPU Utilization**, and then click **Next**.
4. On the **Scope and Counters** page, click the (...) button, and then in the **Select a group or object** dialog box that opens, in the **Filter** box, type **Windows Server**.
5. Under **Available items**, select **Windows Server Computer Group**, and then click **OK**.
6. On the **Scope and Counters** page, click **Add**.
7. In the **Select performance counters** dialog box that opens, under **Object**, select **Processor Information**, and under **Counter**, select **% Processor Time**.
8. Under **Available items**, select **Processor Information**, where the **Performance Instance** column displays **\_Total**, click **Add**, and then click **OK**.
9. On the **Scope and Counters** page, click **Next**.
10. On the **Time Range** page, in the **Last** box, type **5**, change **Hours** to **Days**, and then click **Next**.
11. On the **Chart Preferences** page, click **Next**.
12. On the **Summary** page, click **Create**.
13. On the **Completion** page, click **Close**.

► **Task 5: Configure the third widget**

1. In the **Windows Server Performance** view, click the lower-left **Click** to add widget link.
2. In the New Dashboard and Widget Wizard, on the **Template** page, select **Performance Widget**, and then click **Next**.
3. On the **General Properties** page, in the **Name** box, type **Logical Disk Free Space (%)**, and then click **Next**.
4. On the **Scope and Counters** page, click the (...) button, and then in the **Select a group or object** dialog box that opens, in the **Filter** box, type **Windows Server**.
5. Under **Available items**, select **Windows Server Computer Group**, and then click **OK**.
6. On the **Scope and Counters** page, click **Add**.
7. In the **Select performance counters** dialog box that opens, under **Object**, select **Logical Disk**, and under **Counter**, select **% Free Space**.
8. Under **Available items**, select **LogicalDisk**, where the **Performance Instance** column displays **C:**, click **Add**, and then click **OK**.
9. On the **Scope and Counters** page, click **Next**.
10. On the **Time Range** page, in the **Last** box, type **5**, change **Hours** to **Days**, and then click **Next**.
11. On the **Chart Preferences** page, click **Next**.
12. On the **Summary** page, click **Create**.
13. On the **Completion** page, click **Close**.

► **Task 6: Configure the fourth widget**

1. In the **Windows Server Performance** view, click the lower-right **Click** to add widget link.
2. In the New Dashboard and Widget Wizard, on the **Template** page, select **Performance Widget**, and then click **Next**.

3. On the **General Properties** page, in the **Name** box, type **Processor Queue Length**, and then click **Next**.
4. On the **Scope and Counters** page, click the (...) button, and then in the **Select a group or object** dialog box that opens, in the **Filter** box, type **Windows Server**.
5. Under **Available items**, select **Windows Server Computer Group**, and then click **OK**.
6. On the **Scope and Counters** page, click **Add**.
7. In the **Select performance counters** dialog box that opens, under **Object**, select **System**, and under **Counter**, select **Processor Queue Length**.
8. Under **Available items**, select **System**, where the **Performance Instance** column is blank, click **Add**, and then click **OK**.
9. On the Scope and Counters page, click **Next**.
10. On the **Time Range** page, in the **Last** box, type **5**, change **Hours** to **Days**, and then click **Next**.
11. On the **Chart Preferences** page, click **Next**.
12. On the **Summary** page, click **Create**.
13. On the **Completion** page, click **Close**.

► **Task 7: Export the Management Pack**

1. Create a folder on the drive C named **Export**.
2. In the Operations console, click the **Administration** pane, and then click **Management Packs**.
3. From the list of **Management Packs**, right-click **Windows Server Performance Dashboard**, and then click **Export Management Pack**.
4. In the **Browse For Folder** window that opens, on drive C, select the **Export** folder, and then click **OK**.
5. In the **Operations Manager** pop-up dialog box, click **OK**.

► **Task 8: Copy the GTM tool files and run the tool against the Management Pack**

1. Browse to **\LON-DC1\Media**, and then copy the **GTMTool** folder to the **C:\Export** folder on LON-MS1.
2. Open a Command Prompt window, and change to the **C:\Export\GTMTool\GTMTool** folder.
3. Type the following, and then press **Enter**.

```
GTMTool.exe /SRC C:\Export\Windows.Server.Performance.Dashboard.xml /SRV LON-MS1 /OUT
C:\
```

4. In the **GTM Tool Credential Request** dialog box that opens, in the **User name** box, type **Contoso\Administrator**; in the **Password** box, type **Pa\$\$w0rd**; and then click **OK**.
5. When you receive the message **Do you want to create a Task Pane Dashboard?**, type **N**, and then press Enter.
6. When you receive the message **MP Name or Enter**, type **Microsoft.Windows.Server.Library**, and then press Enter.
7. Wait for the **Health Monitoring** item to appear, type **Microsoft Windows Server**, and then press **Enter**.

Notice the folder where the Management Pack is saved. This is usually **C:\Folder\_0**.

8. Close the **Command** message window.

► **Task 9: Import the Management Pack and view the custom dashboard**

1. In the Operations console, click the **Administration** pane, and then click **Management Packs**.
2. From the **Tasks** pane, click **Import Management Packs**.
3. In the **Import Management Packs** dialog box that opens, click **Add**, and then click **Add from disk**.
4. In the **Online Catalog Connection** window that opens, click **No**.
5. Browse to the folder where the **Management Pack** is saved, click the **Windows.Server.Performance.Dashboard.xml** file, and then click **Open**.
6. Click **Install**, and when the **Management Pack** is imported, click **Close**.
7. Click the **Monitoring** pane, and then expand the **Microsoft Windows Server** folder.
8. Click the **Windows Server Performance** dashboard view, and confirm that the widgets display the relevant data.

**Results:** After this exercise, you should have created a new Management Pack and dashboard view by using the Grid template. You should have also configured the four widgets to display the performance counters for all Windows Servers. Then, you exported the Management Pack and used the GTM tool utility to import the Management Pack into the Microsoft Windows Server folder. Finally, you imported the Management Pack, viewed the dashboard, and confirmed that the widgets displayed the correct data.

## Module 8: Configuring and Customizing the Operations Console

# Lab: Customizing the Operations Console

### Exercise 1: Creating User Roles and importing the Active Directory Management Packs

#### ► Task 1: Import the Active Directory management packs

1. On LON-MS1 click **Start**, then type **Shell** then click **Operations Manager Shell**.
2. In the **Administrator: Operations Manager Shell** window that opens type the following command and then press **Enter**.

```
CD ADMPS
```

3. Type the following command and then press **Enter**.

```
.\ImportADMPs.ps1
```

4. Wait for the command to complete and then close the Administrator: **Operations Manager Shell** window.

#### ► Task 2: Create a user role for the SQL Server support team

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, expand **Security**, and then click **User Roles**.
3. Right-click **User Roles**, click **New User Role**, and then click **Operator**.
4. In the **Create User Role Wizard – Operator Profile** dialog box that opens, on the **General Properties** page, in the **User role name** box, type **SQL Administrators**, and then under **User role members**, click **Add**.
5. In the **Select Users or Groups** dialog box that opens, in the **Enter the object names to select** box, type **SQL\_Admns**, and then click **Check Names**.
6. In the **Select Users or Groups** dialog box, click **OK**.
7. On the **General Properties** page, click **Next**.
8. On the **Group Scope** page, clear the **SCOM2012** check box, select all groups that are prefixed with **SQL**, and then click **Next**.
9. On the **Tasks** page, select **Only tasks explicitly added to the 'Approved tasks' grid are approved**, and then click **Add**.
10. In the **Select Tasks** dialog box that opens, click the **Management Pack** column header to sort by Management Pack.
11. Multiselect all tasks that belong to Management Packs that are prefixed with **SQL**, and then click **OK**.
12. Click **Next**.
13. On the **Dashboards and Views** page, select **Only the dashboards and views selected in each tab are approved**.
14. On the **Monitoring Tree** tab, select **Microsoft SQL Server** and In the **Warning** dialog box that opens, click **OK**.

15. Ensure all subfolders and views are automatically selected and then click **Next**.
  16. In the **Approving specific views** dialog box that opens, click **OK**.
  17. On the **Summary** page, click **Create**.
  18. In the **User Roles** node, confirm the **SQL Administrators User Role** is visible.
- **Task 3: Create a user role for the Active Directory support team**
1. On LON-MS1, open the Operations console.
  2. Click the **Administration** pane, expand **Security**, and then click **User Roles**.
  3. Right-click **User Roles**, click **New User Role**, and then click **Operator**.
  4. In the **Create User Role Wizard – Operator Profile** dialog box that opens, on the **General Properties** page, in the **User role name** box, type **AD Administrators**, and then under **User role members**, click **Add**.
  5. In the **Select Users or Groups** dialog box that opens, in the **Enter the object names to select** box, type **AD\_Admins**, and then click **Check Names**.
  6. In the **Select Users or Groups** dialog box, click **OK**.
  7. On the **General Properties** page, click **Next**.
  8. On the **Group Scope** page, clear the **SCOM2012** check box, and then select the following groups:
    - **Active Directory Topology Root**
    - **AD Domain Controller Group (Windows 2000 Server)**
    - **AD Domain Controller Group (Windows 2003 Server)**
    - **AD Domain Controller Group (Windows Server 2008 and above)**
    - **AD Monitoring Client Computer Group**
  9. Click **Next**.
  10. On the **Tasks** page, select **Only tasks explicitly added to the ‘Approved tasks’ grid are approved**, and then click **Add**.
  11. In the **Select Tasks** dialog box that opens, click the **Management Pack** column header to sort by Management Pack.
  12. Multiselect all tasks that belong to Management Packs that begin with **Active Directory**, and then click **OK**.
  13. Click **Next**.
  14. On the **Dashboards and Views** page, select **Only the dashboards and views selected in each tab are approved**.
  15. On the **Monitoring Tree** tab, select **Microsoft Windows Active Directory**, and then in the **Warning** window that opens click **OK**.
  16. Ensure all subfolders and views are automatically selected and then click **Next**.
  17. In the **Approving specific views** dialog box that opens, click **OK**.
  18. On the **Summary** page, click **Create**.
  19. In the **User Roles** node, confirm the **AD Administrators User Role** is visible.

► **Task 4: Test user role functionality**

1. On LON-MS1, close the **Operations console** if it is already open.
2. Click **Start** and type **Operations**.
3. Right Click **Operations Console** and then click **Open file location**.
4. In the **Operations Manager** window that opens right-click **Operations Console** and then click **Send to** and then click **Desktop (create shortcut)**.
5. Close the **Operations Manager** window.
6. Hold down the **Shift** key on the keyboard, and then right-click the **Operations console** icon on the desktop.
7. Click **Run as different user**.
8. In the **Windows Security** dialog box that opens, in the **User name** box, type **Contoso\adadmin**.
9. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
10. In the **Operations console** that opens, click the **Monitoring** pane, and then confirm that only the **Microsoft Windows Active Directory** folder is visible.
11. Expand **Microsoft Windows Active Directory**, and then click **DC State**.
12. Confirm that only **LON-DC1.CONTOSO.COM** is visible in the details pane.
13. Click **DC Active Alerts**.
14. Confirm there are no alerts that do not relate to **Active Directory** displayed.
15. Close the Operations console.
16. Hold down the Shift on the keyboard, and then right-click the **Operations console** icon on the desktop.
17. Click **Run as different user**.
18. In the **Windows Security** window that opens, in the **User name** box, type **Contoso\sqladmin**.
19. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
20. In the Operations console that opens, click the **Monitoring** pane, and then confirm that only the **Microsoft SQL Server** folder is visible.
21. Expand the **Microsoft SQL Server** folder, and then click **Computers**.
22. Confirm that only **LON-AP1.CONTOSO.COM**, **LON-AP2.CONTOSO.COM**, **LON-SQ1.CONTOSO.COM** and **LON-SC1.CONTOSO.COM** are displayed in the details pane.
23. Click **Active Alerts**, and then confirm that only alerts related to Microsoft SQL Server are displayed in the details pane (if any alerts appear).
24. Close the Operations console.

**Results:** After this exercise, you should have created a User Role in Operations Manager for the Active Directory support team and the SQL Server support team. You should have also confirmed that the Operations console is scoped appropriately by opening the console as a member of each team.

## Exercise 2: Creating Custom Resolution States

### ► Task 1: Create an alert resolution state for the SQL team

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, and then click **Settings**.
3. From the details pane, double-click **Alerts**.
4. In the **Global Management Group Settings – Alerts** dialog box that opens, on the **Alert Resolution States** tab, click **New**,
5. In the **Add Alert Resolution State** dialog box that opens, in the **Resolution state** box, type **SQL Server Support**.
6. Next to **Unique ID**, click the drop-down list, and then click **30** and then click **OK**.
7. Confirm that **SQL Server Support** is displayed in the **Global Management Group Settings – Alerts** dialog box, and then click **OK**.

### ► Task 2: Create an alert resolution state for the Active Directory team

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, and then click **Settings**.
3. From the details pane, double-click **Alerts**.
4. In the **Global Management Group Settings – Alerts** dialog box that opens, on the **Alert Resolution States** tab, click **New**.
5. In the **Add Alert Resolution State** dialog box that opens, in the **Resolution state** box, type **Active Directory Support**.
6. Next to **Unique ID**, click the drop-down list, and then click **50** and then click **OK**.
7. Confirm the **Active Directory Support** is displayed in the **Global Management Group Settings – Alerts** dialog box, and then click **OK**.

### ► Task 3: Test the alert resolution states

1. On LON-MS1, open the Operations console.
2. Click the **Monitoring** pane, and then click **Active Alerts**.
3. From the details pane, right-click an alert that is associated to either LON-SQ1 or LON-AP2, and then click **Set Resolution State**.
4. Click **SQL Server Support**.
5. Notice the **Resolution State** column for the selected alert now displays **SQL Server Support**.
6. Right-click an alert that is associated with LON-DC1, and then click **Set Resolution State**.
7. Click **Active Directory Support**.
8. Notice the **Resolution State** column for the selected alert now displays **Active Directory Support**.

**Results:** After this exercise, you should have created an alert resolution state for both the SQL Server and Active Directory support teams. You should have also tested the alert resolutions states by assigning alerts to the relevant teams.

## Exercise 3: Creating Custom Views

### ► Task 1: Create the Management Packs

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, and then click **Management Packs**.
3. From the **Tasks** pane, click **Create Management Pack**.
4. In the Create a Management Pack wizard that opens, on the **General Properties** page, in the **Name** box, type **SQL Server Support Team Views**, and then click **Next**.
5. On the **Knowledge** page, click **Create**.
6. From the **Tasks** pane, click **Create a Management Pack**.
7. In the **Create a Management Pack** wizard that opens, on the **General Properties** page, in the **Name** box, type **Active Directory Support Team Views**, and then click **Next**.
8. On the **Knowledge** page, click **Create**.

### ► Task 2: Create Event views

1. On LON-MS1, open the Operations console.
2. Click the **Monitoring** pane, and then click **SQL Server Support Team Views**.
3. Right-click **SQL Server Support Team Views**, click **New**, and then click **Event View**.
4. In the **Properties** window that opens, in the **Name** box, type **SQL Server Events**.
5. Next to the **Show data related to** box, click the **ellipsis** button (...).
6. In the **Select Items to Target** window that opens, in the **Look for** box, type **SQL**.
7. In the details pane, click **SQL DB Engine**, and then click **OK**.
8. Next to the **Show data contained in a specific group** box, click (...).
9. In the **Select Object** window that opens, in the **Text string** box, type **SQL**.
10. In the **Matching objects** window, click **SQL Computers**, and then click **OK**.
11. In the **Properties** window, click **OK**.
12. Click the **Monitoring** pane, and then click **Active Directory Support Team Views**.
13. Right-click **Active Directory Support Team Views**, click **New**, and then click **Event View**.
14. In the **Properties** window that opens, in the **Name** box, type **Active Directory Events**.
15. Next to the **Show data related to** box, click (...).
16. In the **Select Items to Target** window that opens, in the **Look for** box, type **Active**.
17. In the details pane, click **Active Directory DC and Global Catalog Server Role (Windows Server 2008 and above)**, and then click **OK**.
18. Next to the **Show data contained in a specific group** box, click (...).
19. In the **Select Object** window that opens, in the **Text string** box, type **Domain**.
20. In the **Matching objects** window, click **AD Domain Controller Group (Windows Server 2008 and above)**, and then click **OK**.
21. In the **Properties** window, click **OK**.

► **Task 3: Create Performance views**

1. On LON-MS1, open the Operations console.
2. Click the **Monitoring** pane, and then click **SQL Server Support Team Views**.
3. Right-click **SQL Server Support Team Views**, click **New**, and then click **Performance View**.
4. In the **Properties** window that opens, in the **Name** box, type **SQL Server Performance**.
5. Next to the **Show data related to** box, click (...).
6. In the **Select Items to Target** window that opens, in the **Look for** box, type **SQL**.
7. In the details pane, click **SQL DB Engine**, and then click **OK**.
8. Next to the **Show data contained in a specific group** box, click (...).
9. In the **Select Object** window that opens, in the **Text string** box, type **SQL**.
10. In the **Matching objects** window, click **SQL Computers**, and then click **OK**.
11. In the **Properties** window, click **OK**.
12. Click the **Monitoring** pane, and then click **Active Directory Support Team Views**.
13. Right-click **Active Directory Support Team Views**, click **New**, and then click **Performance View**.
14. In the **Properties** window that opens, in the **Name** box, type **Active Directory Performance**.
15. Next to the **Show data related to** box, click (...).
16. In the **Select Items to Target** window that opens, in the **Look for** box, type **Active**.
17. In the details pane, click **Active Directory DC and Global Catalog Server Role (Windows Server 2008 and above)**, and then click **OK**.
18. Next to the **Show data contained in a specific group** box, click (...).
19. In the **Select Object** window that opens, in the **Text string** box, type **Domain**.
20. In the **Matching objects** window, click **AD Domain Controller Group (Windows Server 2008 and above)**, and then click **OK**.
21. In the **Properties** window, click **OK**.

► **Task 4: Create Alert views**

1. On LON-MS1, open the Operations console.
2. Click the **Monitoring** pane, and then click **SQL Server Support Team Views**.
3. Right-click **SQL Server Support Team Views**, click **New**, and then click **Alert View**.
4. In the **Properties** window that opens, in the **Name** box, type **Alerts Assigned to SQL Server Support**.
5. Under **Select conditions**, select **with specific resolution state**.
6. Under **Criteria description (click the underlined value to edit)**, click **specific**.
7. In the **Resolution State** window that opens, select **SQL Server Support (30)**, and then click **OK**.
8. In the **Properties** window, click **OK**.
9. Right-click **Active Directory Support Team Views**, click **New**, and then click **Alert View**.
10. In the **Properties** window that opens, in the **Name** box, type **Alerts Assigned to Active Directory Support**.

11. Under **Select conditions**, select **with a specific resolution state**.
12. Under **Criteria description (click the underlined value to edit)**, click **specific**.
13. In the **Resolution State** window that opens, select **Active Directory Support (50)**, and then click **OK**.
14. In the **Properties** window, click **OK**.

► **Task 5: Create Diagram views**

1. On LON-MS1, open the Operations console.
2. Click the **Monitoring** pane, and then click **SQL Server Support Team Views**.
3. Right-click **SQL Server Support Team Views**, click **New**, and then click **Diagram View**.
4. In the **Create Diagram View** window that opens, in the **Name** box, type **SQL Server Components**.
5. Click **Browse**, and in the **Object Search** window that opens, in the **Filter by** box, type **SQL**, and then click **Search**.
6. Under **Available items**, click **SQL Components**, click **Add**, and then click **OK**.
7. Select **Create your own template**; in the **Levels to Show** box, increase the **Levels to Show** value from **2** to **4**; and then click **Create**.
8. In the **Operations Manager** window that opens, click **Yes**.
9. Click the **Monitoring** pane, and then click **Active Directory Support Team Views**.
10. Right-click **Active Directory Support Team Views**, click **New**, then click **Diagram View**.
11. In the **Create Diagram View** window that opens, in the **Name** box, type **Active Directory Components**.
12. Click **Browse**, and in the **Object Search** window that opens, in the **Filter by** box, type **domain**, and then click **Search**.
13. Under **Available items**, click **AD Domain Controller Group (Windows Server 2008 and above)**, click **Add**, and then click **OK**.
14. Select **Create your own template**; in the **Levels to Show** box, increase the **Levels to Show** value from **2** to **4**; and then click **Create**.

► **Task 6: Update the user roles to include the new views**

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane.
3. Expand **Security**, and then click **User Roles**.
4. From the details pane, right-click **SQL Administrators**, and then click **Properties**.
5. In the **SQL Administrators – User Role Properties** window that opens, click the **Dashboards and Views** tab.
6. In the **Monitoring Tree** tab, select **Microsoft SQL Server**, and ensure all subfolders and views are also selected.
7. In the **Warning** window that opens, click **OK**.
8. Select **SQL Server Support Team Views**, and ensure all subviews are also selected.
9. Click **OK**.

10. In the **Approving specific views** window that opens, click **OK**.
  11. From the details pane, right-click **AD Administrators**, and then click **Properties**.
  12. In the **AD Administrators – User Role Properties** window that opens, click the **Dashboards and Views** tab.
  13. In the **Monitoring Tree** tab, select **Microsoft Windows Active Directory**, and ensure all subfolders and views are also selected.
  14. In the **Warning** window that opens, click **OK**.
  15. Select **Active Directory Support Team Views**, and ensure all subviews are also selected.
  16. Click **OK**.
  17. In the **Approving specific views** window that opens, click **OK**.
- **Task 7: Confirm the new views are available in the scoped consoles**
1. On LON-MS1, close the Operations console if it is already open.
  2. Hold down the Shift key, and then right-click the **Operations console** icon on the desktop.
  3. Click **Run as different user** and then in the **Windows Security** window that opens type **Contoso\sqladmin** in the **User name** box.
  4. Type **Pa\$\$w0rd** in the **Password** box and then click **OK**.
  5. In the **Operations console** confirm only the **Microsoft SQL Server** and **SQL Server Support Team Views** folders are available.
  6. Expand **SQL Server Support Team Views** and then open the following views:
    - Alerts Assigned to SQL Server Support
    - SQL Server Components
    - SQL Server Events
    - SQL Server Performance
  7. Close the Operations console.
  8. Hold down the Shift key, and then right-click the **Operations console** icon on the desktop.
  9. Click **Run as different user**, and then in the **Windows Security** window that opens, in the **User name** box, type **Contoso\adadmin**.
  10. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
  11. In the Operations console, confirm that only the **Microsoft Windows Active Directory** and **Active Directory Support Team Views** are available.
  12. Expand **Active Directory Support Team Views**, and then open the following views:
    - Active Directory Components
    - Active Directory Events
    - Active Directory Performance
    - Alerts Assigned to Active Directory Support
  13. Close the Operations console.

**Results:** After this exercise, you should have created custom views for both the SQL Server support team and Active Directory support team. These views include Events, Performance Counters, Alerts, and Diagrams for the respective teams.

## Exercise 4: Configuring Notifications

### ► Task 1: Configure an SMTP notification channel

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, and then expand **Notifications**.
3. Click **Channels**, and then from the **Tasks** pane, click **New**, and then click **E-Mail (SMTP)**.
4. In the E-Mail Notification Channel wizard, on the **Description** page, click **Next**.
5. On the **Settings** page, click **Add**.
6. In the **Add SMTP Server** window that opens, in the **SMTP Server (FQDN)** box, type **LON-AP1.contoso.com**.
7. Under **Authentication method**, click the drop-down menu, click **Windows Integrated**, and then click **OK**.
8. In the **Return address** box, type **Administrator@Contoso.com**, and then click **Next**.
9. On the **Format** page, click **Finish**, and then click **Close**.
10. Logon to LON-AP1, click **Start** and then click **Administrative Tools** and then double-click **Internet Information Services (IIS) 6.0 Manager**.
11. In the **Internet Information Services (IIS) 6.0 Manager** window that opens expand **LON-AP1 (local computer)** and then right-click **[SMTP Virtual Server #1]** and then click **Start**.
12. Close **Internet Information Services (IIS) 6.0 Manager** and then log off LON-AP1.

### ► Task 2: Configure a notification subscriber for the Active Directory and SQL Server support teams

1. Logon to LON-MS1 and then open the **Operations console**,
2. Click the **Administration** pane, and then expand **Notifications**.
3. Click **Subscribers**, and from the **Tasks** pane, click **New**.
4. In the Notifications Subscriber Wizard, on the **Description** page, in the **Subscriber Name** box, type **SQLAdmin**, and then click **Next**.
5. On the **Schedule** page, click **Next**.
6. On the **Addresses** page, click **Add**.
7. In the **Subscriber Address** wizard, on the **General** page, in the **Address name** box, type **SQLAdmin**, and then click **Next**.
8. On the **Channel** page, click the **Channel type** drop-down list, and then click **E-Mail (SMTP)**.
9. In the **Delivery address for the selected channel** box, type **sqladmin@Contoso.com**, and then click **Next**.
10. On the **Schedule** page, click **Finish**.
11. On the **Addresses** page, click **Finish**, and then click **Close**.
12. From the **Tasks** pane, click **New**.
13. In the Notifications Subscriber Wizard, on the **Description** page, in the **Subscriber Name** box, type **ADAdmin**, and then click **Next**.
14. On the **Schedule** page, click **Next**.

15. On the **Addresses** page, click **Add**.
16. In the **Subscriber Address** wizard, on the **General** page, in the **Address name** box, type **ADAdmin**, and then click **Next**.
17. On the **Channel** page, click the **Channel type** the drop-down list, and then click **E-Mail (SMTP)**.
18. In the **Delivery address for the selected channel** box, type **adadmin@Contoso.com**, and then click **Next**.
19. On the **Schedule** page, click **Finish**.
20. On the **Addresses** page, click **Finish**, and then click **Close**.

► **Task 3: Configure a notification subscription for the Active Directory and SQL Server support teams**

1. On LON-SQ1 and LON-DC1, stop the **Microsoft Monitoring Agent** Service.
2. On LON-MS1, open the Operations console, click the **Monitoring** pane, and then click **Active Alerts**.
3. Wait for the **Health Service Heartbeat Failure** alert for LON-SQ1 to be generated.
4. Right-click the **Health Service Heartbeat Failure** alert for LON-SQ1, click **Notification Subscription**, and then click **Create**.
5. In the Notification Subscription Wizard, on the **Description** page, click **Next**.
6. On the **Criteria** page, under **Conditions**, select **with specific resolution state**, and then under **Criteria** description, click the **specific** link.
7. In the **Resolution State** window that opens, select **SQL Server Support (30)**, and then click **OK**.
8. On the **Criteria** page, click **Next**.
9. On the **Subscribers** page, click **Add**.
10. In the **Subscriber Search** window that opens, click **Search**.
11. Under **Available subscribers**, click **SQLAdmin**, click **Add**, and then click **OK**.
12. On the **Subscribers** page, click **Next**.
13. On the **Channels** page, click **Add**.
14. On the **Channel Search** page, click **Search**.
15. Under **Available channels**, click **E-Mail (SMTP)**, click **Add**, and then click **OK**.
16. On the **Channels** page, click **Next**.
17. On the **Summary** page, click **Finish**, and then click **Close**.
18. Click **Active Alerts**.
19. Wait for the **Health Service Heartbeat Failure** alert for LON-DC1 to be generated.
20. Right-click the **Health Service Heartbeat Failure** alert for LON-DC1, click **Notification Subscription**, and then click **Create**.
21. In the Notification Subscription Wizard, on the **Description** page, click **Next**.
22. On the **Criteria** page, under **Conditions**, select **with specific resolution state**, and then under **Criteria** description, click the **specific** link.
23. In the **Resolution State** window that opens, select **Active Directory Support (50)**, and then click **OK**.

24. On the **Criteria** page, click **Next**.
25. On the **Subscribers** page, click **Add**.
26. In the **Subscriber Search** window that opens, click **Search**.
27. Under **Available subscribers**, click **ADAdmin**, click **Add**, and then click **OK**.
28. On the **Subscribers** page, click **Next**.
29. On the **Channels** page, click **Add**.
30. On the **Channel Search** page, click **Search**.
31. Under **Available channels**, click **E-Mail (SMTP)**, click **Add**, and then click **OK**.
32. On the **Channels** page, click **Next**.
33. On the **Summary** page, click **Finish**, and then click **Close**.

#### ► Task 4: Test notifications

1. On LON-MS1, in the Operations console, click the **Monitoring** pane, and then click **Active Alerts**.
2. Right-click the **Health Service Heartbeat Failure** alert associated with LON-SQ1, and then click **Set Resolution State**.
3. Click **SQL Server Support**.
4. Browse to **\LON-AP1\C\$\InetPub\MailRoot\Drop**
5. Refresh the view until an .eml file appears. This can take up to two minutes.
6. Open the .eml file by using Notepad, and then confirm the alert details have been sent to **SQLAdmin** by viewing the **To** and **Subject** fields.
7. Delete the .eml file.
8. From the **Active Alerts** view in the **Operations console**, right-click the **Health Service Heartbeat Failure** alert associated with LON-DC1, and then click **Set Resolution State**.
9. Click **Active Directory Support**.
10. Browse to **\LON-AP1\C\$\InetPub\MailRoot\Drop**
11. Refresh the view until an .eml file appears. This can take up to two minutes.
12. Open the .eml file by using Notepad, and then confirm the alert details have been sent to **ADAdmin** by viewing the **To** and **Subject** fields.
13. Delete the .eml file.
14. Start the **Microsoft Monitoring Agent** Service on LON-SQ1 and LON-DC1.

**Results:** After this exercise, you should have created a notification subscription for both the SQL Server support team and the Active Directory support team. You should have then tested that email notifications were working by generating an alert and confirming the relevant support teams were notified via email.

## Exercise 5: Configuring Diagnostic and Recovery Tasks

► **Task 1: Create a recovery script**

1. On LON-SQ1 create a file on C named **RestartSQLAgent.bat**.
2. Edit the **RestartSQLAgent.bat** file and add the following text:

```
Net Start SQLSERVERAGENT
```

3. Save the **RestartSQLAgent.bat** file, and then close it.
4. Open **Windows Services** and stop the **SQL Server Agent (MSSQLSERVER)** service.
5. Logoff LON-SQ1.

► **Task 2: Create diagnostic and recovery tasks**

1. On LON-MS1, open the Operations console.
2. Click **Active Alerts**, and then wait for the **SQL Server Agent Windows Stopped** alert to appear.
3. Right-click the alert, and then click **View or edit the settings of this monitor**.
4. In the **SQL Server Agent Windows Service Properties** window that opens, click the **Diagnostic and Recovery** tab.
5. Under **Configure diagnostic tasks**, click **Add**.
6. Click **Diagnostic for critical health state**.
7. In the Create Diagnostic Task Wizard that opens, on the **Diagnostic Task Type** page, click **Run Command**, and then next to **Management Pack**, click **New**.
8. In the Create a Management Pack wizard that opens, on the **General Properties** page, in the **Name** box, type **SQL Agent Monitor Overrides**, and then click **Next**.
9. On the **Knowledge** page, click **Create**.
10. In the Create Diagnostic Task Wizard, on the **Diagnostic Task Type** page, click **Next**.
11. On the **General** page, in the **Diagnostic name** box, type **Return Process List**.
12. Clear **Run diagnostic automatically**, and then click **Next**.
13. On the **Command Line** page, in the **Full path to file** box, type **%windir%\system32\tasklist.exe**, and then click **Create**.
14. In the **Configure diagnostic tasks** section, confirm the **Return Process List** task is displayed.
15. Under **Configure recovery tasks**, click **Add**.
16. Click **Recovery for critical health state**.
17. In the **Create Recovery Task Wizard** that opens, on the **Diagnostic Task Type** page, click **Run Command**, click the **Management Pack** drop-down list, click **SQL Agent Monitor Overrides**, and then click **Next**.
18. On the **General** page, in the **Recovery name** box, type **Restart SQL Agent**.
19. Clear **Run recovery automatically**, and then click **Next**.
20. On the **Command Line** page, in the **Full path to file** box, type **C:\RestartSQLAgent.bat**, and then click **Create**.
21. In the **Configure recovery tasks** section, confirm the **Restart SQL Agent** task is displayed.

22. Close the **SQL Server Agent Windows Service Properties** window.

23. On LON-SQ1, start the **SQL Server Agent (MSSQLSERVER)** service.

► **Task 3: Test diagnostic and recovery tasks**

1. On LON-SQ1, stop the SQL Server Agent (MSSQLSERVER) service.

2. On LON-MS1, open the Operations console.

3. Click **Active Alerts**, and then wait for the **SQL Server Agent Windows Stopped** alert to appear.

4. Right-click the alert, click **Open**, and then click **Health Explorer**.

5. In the **Health Explorer for SQLSERVERAGENT** window that opens, click **SQL Server Agent Windows Service – SQLSERVERAGENT (SQL Server 2012 Agent)**, and then click the **State Change Events** tab.

6. Under **Diagnostic and Recovery Options**, click **Return Process List**.

7. In the **Confirm Action** window that opens, click **Yes**.

8. Wait for the view to update, and then scroll down and review the output that has been appended.

9. Under **Additional Recovery Options**, click **Restart SQL Agent**.

10. In the **Confirm Action** window that opens, click **Yes**.

11. Wait for the view to update, and then scroll down and review the output that has been appended.

12. Close the **Health Explorer for SQLSERVERAGENT** window.

13. On LON-SQ1, confirm the SQL Server Agent (MSSQLSERVER) service has been automatically restarted by the recovery task.

**Results:** After this exercise, you should have created a diagnostic and recovery task in Operations Manager. You should also have tested the diagnostic and recovery tasks in the Operations console.

# Module 9: Management Pack Authoring

## Lab: Authoring Management Packs

### Exercise 1: Creating a Management Pack in the Operations console

#### ► Task 1: Create a Management Pack in the Operations console

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, and then click **Management Packs**.
3. From the **Tasks** pane, click **Create Management Pack**.
4. In the Create a Management Pack wizard that opens, on the **General Properties** page, in the **Name** box, type **DinnerNow Custom Monitoring**, and then click **Next**.
5. On the **Knowledge** page, click **Create**.
6. In the **Management Packs** node, confirm the **DinnerNow Custom Monitoring** Management Pack was created.
7. Click the **Monitoring** pane.
8. Under the **Monitoring** node, confirm the **DinnerNow Custom Monitoring** folder was created.

#### ► Task 2: Create a group to target overrides

1. On LON-MS1, in the **Operations console** click the **Authoring** pane.
2. Click **Groups**, and then from the **Tasks** pane, click **Create a New Group**.
3. In the **Create Group Wizard** that opens, on the **General Properties** page, in the **Name** box, type **DinnerNow Production Servers**.
4. Click the **Management Pack** drop-down list, click **DinnerNow Custom Monitoring**, and then click **Next**.
5. On the **Explicit Members** page, click **Add/Remove Objects**.
6. In the **Create Group Wizard – Object Selection** dialog box that opens, click the **Search for** drop-down list, click **Windows Computer**, and then click **Search**.
7. In the **Available items** section, click **LON-AP2.CONTOSO.COM**, click **Add**, and then click **OK**.
8. On the **Explicit Members** page, click **Next**.
9. On the **Dynamic Members** page, click **Next**.
10. On the **Subgroups** page, click **Next**.
11. On the **Excluded Members** page click **Create**.
12. From the **Groups** node, right-click **DinnerNow Production Servers**, and then click **View Group Members**.
13. In the **Managed Objects – SCOM2012 – Operations Manager** window that opens, confirm **LON-AP2.CONTOSO.COM** is displayed, and then close the **Managed Objects – SCOM2012 – Operations Manager** window.

#### ► Task 3: Create monitors for the application

1. On LON-MS1, in the Operations console, click the **Authoring** pane.
2. Expand **Management Pack Objects**, and then click **Monitors**.

3. From the **Tasks** pane, click **Create a Monitor**, and then click **Unit Monitor**.
  4. In the Create a unit monitor wizard that opens, on the **Monitor Type** page, expand **Windows Performance Counters**, expand **Static Thresholds**, expand **Single Threshold**, and then click **Simple Threshold**.
  5. Click the **Management Pack** drop-down list, click **DinnerNow Custom Monitoring**, and then click **Next**.
  6. On the **General** page, in the **Name** box, type **DinnerNow Database Server CPU Utilization**.
  7. Next to **Monitor target**, click **Select**.
  8. In the **Select Items to Target** dialog box that opens, type **Windows Server 2008 Operating System**.
  9. In the details section, click **Windows Server 2008 Operating System**, and then click **OK**.
  10. Under **Parent monitor**, click the drop-down list, and then click **Performance**.
  11. Clear the **Monitor is enabled** check box, and then click **Next**.
  12. On the **Performance Counter** page, click **Select**.
  13. In the **Select Performance Counter** window that opens, click the **Object** drop-down list, and then click **Processor Information**.
  14. In the **Select counter from list** section, click **% Processor Time**, and then click **OK**.
  15. In the **Interval** box, remove **15** and type **5**, and then click **Next**.
  16. On the **Threshold Value** page, in the **Threshold Value** box, remove **0.00** and type **10.00**, and then click **Next**.
  17. On the **Configure Health** page, click **Next**.
  18. On the **Configure Alerts** page, select the **Generate alerts for this monitor** check box.
  19. Clear the **Automatically resolve the alert when the monitor returns to a healthy state** check box, and then click **Create**.
- **Task 4: Create rules for the application**
1. On LON-MS1, in the Operations console, click the **Authoring** pane.
  2. Expand **Management Pack Objects**, and then click **Rules**.
  3. From the **Tasks** pane, click **Create a Rule**.
  4. In the Create Rule Wizard that opens, on the **Rule Type** page, under the **Alert Generating Rules** section, expand **Event Based**, and then click **NT Event Log (Alert)**.
  5. Click the **Management Pack** drop-down list, and then click **DinnerNow Custom Monitoring**, and then click **Next**.
  6. On the **General** page, in the **Rule name** box, type **DinnerNow Database Unavailable**.
  7. Next to **Rule target**, click **Select**.
  8. In the **Select Items to Target** dialog box that opens, in the **Look for** box, type **Windows Server 2008 Operating System**.
  9. In the details section, click **Windows Server 2008 Operating System**, and then click **OK**.
  10. Clear the check-box for **Rule is enabled**, and then click **Next**.
  11. On the **Event Log Type** page, click **Next**.

12. On the **Build Event Expression** page, in the **Value** box for **Event ID**, type **5084**.
13. In the **Value** box for **Event Source**, type **MSSQL\$SQLEXPRESS**, and then click **Next**.
14. On the **Configure Alerts** page, click **Alert suppression**.
15. In the **Alert Suppression** dialog box that opens, select the **Event ID** check box, and then click **OK**.
16. Click **Create**.

► **Task 5: Create overrides to adjust monitoring thresholds**

1. On LON-MS1, in the Operations console, click the **Authoring** pane.
2. Expand **Management Pack Objects**, and then click **Monitors**.
3. If a scope is applied to the **Monitors** view, click the **x** to remove the scope.
4. In the **Look for** box, type **DinnerNow Database Server CPU Utilization**, and then click **Find Now**.
5. From the list of returned objects, expand **Windows Server 2008 Operating System**, expand **Entity Health**, expand **Performance**, and then right-click **DinnerNow Database Server CPU Utilization**.
6. Click **Overrides**, click **Override the Monitor**, and then click **For a group**.
7. In the **Select Object** window that opens, click **DinnerNow Production Servers**, and then click **OK**.
8. In the **Override Properties** window that opens, select the **Override** check box for the **Enabled** parameter, and then change the **Override Value** from **False** to **True**.
9. Select the **Override** check box for the **Threshold** parameter, and then in the **Override Value** box, remove **10** and type **5**.
10. In the **Overrides Properties** window, click **OK**.
11. Under **Management Pack Objects**, click **Rules**.
12. If a scope is applied to the **Rules** view, click the **x** to remove the scope.
13. In the **Look for** box, type **DinnerNow Database Unavailable**, and then click **Find Now**.
14. From the list of returned objects, expand **Windows Server 2008 Operating System**, and then right-click **DinnerNow Database Unavailable**.
15. Click **Overrides**, click **Override the Rule**, and then click **For a group**.
16. In the **Select Object** window that opens, click **DinnerNow Production Servers**, and then click **OK**.
17. In the **Override Properties** window that opens, select the **Override** check box for the **Enabled** parameter, and then change the **Override Value** from **False** to **True**.
18. In the **Overrides Properties** window, click **OK**.

► **Task 6: Create monitoring views**

1. On LON-MS1, in the Operations console, click the **Monitoring** pane.
2. Right-click the **DinnerNow Custom Monitoring** folder, click **New**, and then click **Alert View**.
3. In the **Properties** window that opens, in the **Name** box, type **DinnerNow Database Unavailable Alerts**.
4. Next to the **Clear** button, click the **ellipsis** button (...).
5. In the **Select Object** window that opens, click **DinnerNow Production Servers**, and then click **OK**.
6. In the **Select conditions** section, select the **with a specific name** check box.
7. In the **Criteria description** section, click the **specific** link.

8. In the **Alert Name** window that opens, in the **Text String** box, type **DinnerNow Database Unavailable**, and then click **OK**.
9. In the **Properties** window, click **OK**.
10. Wait for the view to be created.
11. Right-click the **DinnerNow Custom Monitoring** folder, click **New**, and then click **Alert View**.
12. In the **Properties** window that opens, in the **Name** box, type **DinnerNow Database Server CPU Utilization High Alerts**.
13. Click (...) next to the **Clear** button.
14. In the **Select Object** window that opens, click **DinnerNow Production Servers**, and then click **OK**.
15. In the **Select conditions** section, select the **with a specific name** check box.
16. In the **Criteria description** section, click the **specific** link.
17. In the **Alert Name** window that opens, in the **Text String** box, type **DinnerNow Database Server CPU Utilization**, and then click **OK**.
18. In the **Properties** window, click **OK**.
19. Wait for the view to be created.

#### ► Task 7: Test monitoring views

1. Log on to LON-AP2, and from the desktop, double-click **DinnerNow SQL DBDetatcher**.
2. In the **SQL Stop Start** window that opens, click **Stop**.
3. Leave the **SQL Stop Start** window open.
4. On LON-MS1, in the Operations console, click the **Monitoring** pane, and then expand **DinnerNow Custom Monitoring**.
5. Click **DinnerNow Database Unavailable Alerts**.
6. From the details pane, notice that the **DinnerNow Database Unavailable** alert has been generated.
7. Double-click the alert, and in the **Alert Properties** window that opens, click the **General** tab.
8. Notice the **Repeat Count** value of **0**.
9. Close the **Alert Properties** window.
10. On LON-AP2, in the **SQL Stop Start** window, click **Start**.
11. Wait approximately five seconds, and then click **Stop**.
12. On LON-MS1, in the Operations console, double-click the **DinnerNow Database Unavailable** alert.
13. In the **Alert Properties** window, on the **General** tab, notice that the **Repeat Count** value has increased to **1**.



**Note:** It may take up to 5 minutes for the repeat count to increase.

14. Close the **Alert Properties** window.
15. On LON-AP2, in the **SQL Stop Start** window, click **Start**.
16. On LON-MS1, in the Operations console, click the **DinnerNow Database Server CPU Utilization High Alerts** view.

17. From the details pane, notice the **DinnerNow Database Server CPU Utilization** alert has been generated.
18. Right-click the alert, click **Open**, and then click **Health Explorer**.
19. In the **Health Explorer for Microsoft Windows Server 2008 R2 Enterprise** window that opens, click **Entity Health – Microsoft Windows Server 2008 R2 Enterprise (Object)**.
20. Click the **State Change Events** tab.
21. Review the state change events and details for the monitor.
22. Close the **Health Explorer for Microsoft Windows Server 2008 R2 Enterprise** window.

**Results:** After this exercise, you should have created a new Management Pack for DinnerNow by using the Operations console. You should have then created a group to target specific computers that host the DinnerNow components. Next, you should have created a rule and monitor for DinnerNow, and created an override to adjust the monitoring thresholds for the DinnerNow application.

## Exercise 2: Authoring a Management Pack by Using Visual Studio Authoring Extensions

### ► Task 1: Create the new Management Pack

1. Logon to LON-AP1, click **Start** and then type **Visual Studio** then click **Visual Studio Tools**.
2. In the **Shortcuts** window that opens double-click **VS2013 x64 Native Tools Command Prompt**.
3. In the **Administrator: VS2013 x64 Native Tools Command Prompt** window that opens type the following and then press enter on the keyboard:

```
CD "C:\Program Files (x86)\Microsoft Visual Studio
12.0\Common7\IDE\CommonExtensions\Microsoft\Editor"
```

4. Type the following command and then press enter on the keyboard:

```
gacutil /i Microsoft.VisualStudio.Text.Logic.dll
```

5. Close the **Administrator: VS2013 x64 Native Tools Command Prompt** window

6. Create the following folder structure on the C drive:

```
C:\Temp\DinnerNow\2012TMP
```

7. From the desktop double-click **Visual Studio 2013**.
8. In **Visual Studio**, click the **File** menu, click **New**, and then click **Project**.
9. In the **New Project** window that opens, click **Management Pack**, and then click **Operations Manager 2007 R2 Management Pack**.
10. In the **Name** box, type **CONTOSO.DinnerNow**.
11. In the **Location** box, type **C:\Temp\DinnerNow\2012TMP**.
12. Click **OK**.
13. Click the **View** menu and then click **Solution Explorer**.
14. In the **Solution Explorer** pane, right-click **CONTOSO.DinnerNow**, and then click **Properties**.
15. In the **CONTOSO.DinnerNow** window that opens, click the **Management Group** tab, and then click **Add**.
16. In the **Add Management Server** window that opens, in the **Server Name** box, type **LON-MS1**, and then click **Test Connection** then click **Add Server**.
17. Right-click the **CONTOSO.DinnerNow** tab, and then click **Save Selected Items**.
18. Close the **CONTOSO.DinnerNow** window.
19. In the **Solution Explorer** pane, right-click **CONTOSO.DinnerNow**, click **Add**, and then click **New Folder**.
20. Rename the folder to **Classes**.
21. Repeat steps 19 and 20 to create the following folders:
  - **Discoveries**
  - **Modules and Types**
  - **Monitors**
  - **Rules**

- **Views**

22. Right-click **References**, and then click **Add Reference**.
  23. In the **Add Reference** window that opens, click the **Browse** tab; in the **File name** box, type **\LON-DC1\Media\Additional Management Packs**; and then press Enter on the keyboard.
  24. Open the SQL Server folder and then click **Microsoft.SQLServer.Library.mp** and then click **OK**.
  25. Repeat steps 23 – 25 to add references for the following Management Packs:
    - **Microsoft.Windows.InternetInformationServices.2008.mp** from the **\LON-DC1\Media\Additional Management Packs\Internet Information Services 7** folder.
    - **Microsoft.Windows.InternetInformationServices.CommonLibrary.mp** from the **\LON-DC1\Media\Additional Management Packs\Internet Information Services 7** folder.
  26. Right-click **References** again, and then click **Add Reference**.
  27. In the **Add Reference** window that opens, click the **Browse** tab, and then browse to **C:\Program Files (x86)\System Center 2012 Visual Studio Authoring Extensions\References\OM2007R2**.
  28. Hold down the Ctrl key, multiselect the following files, and then click **OK**:
    - **Microsoft.SystemCenter.DataWarehouseLibrary.mp**
    - **System.Performance.Library.mp**
  29. In Solution Explorer, under **References**, click **Microsoft.SQLServer.Library**.
  30. In the **Properties** window, in the **Alias** box, remove the existing text, and then type **SQL**.
  31. In Solution Explorer, under **References**, click  
**Microsoft.Windows.InternetInformationServices.2008**.
  32. In the **Properties** window, in the **Alias** box, remove the existing text, and then type **IIS2008**.
  33. In Solution Explorer, under **References**, click  
**Microsoft.Windows.InternetInformationServices.CommonLibrary**.
  34. In the **Properties** window, in the **Alias** box, remove the existing text, and then type **IIS**.
- **Task 2: Define the service model**
1. Right-click the **Classes** folder, click **Add**, and then click **New Item**.
  2. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Class**.
  3. In the **Name** box, remove the existing text, type **Application.Class.mpx**, and then click **Add**.
  4. In the line that starts with **ClassType ID= “CONTOSO.DinnerNow.Application”**, change the **Base** element to **“Windows!Microsoft.Windows.LocalApplication”**.
  5. Change the **Hosted** element to **“true”**.
  6. In between the line that displays **-- >**, and the line that displays **<ClassType>**add the following four lines of XML code.

```

<Property ID="InstallPath" Key="false" Type="string" CaseSensitive="false"
MinLength="0" MaxLength="256"></Property>
<Property ID="DatabasePath" Key="false" Type="string" CaseSensitive="false"
MinLength="0" MaxLength="256"></Property>
<Property ID="Website" Key="false" Type="string" CaseSensitive="false" MinLength="0"
MaxLength="256"></Property>
<Property ID="DatabaseName" Key="false" Type="string" CaseSensitive="false"
MinLength="0" MaxLength="256"></Property>

```

7. In between the line that displays -- >, and the line that displays </DisplayStrings> add the following four lines of XML code.

```
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="InstallPath">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="DatabasePath">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="Website">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
<DisplayString ElementID="CONTOSO.DinnerNow.Application" SubElementID="DatabaseName">
 <Name>Install Path</Name>
 <Description></Description>
</DisplayString>
```

8. In the four <Name>Install Path</Name> sections replace **Install Path** with the following starting from the first:
- Install Path
  - Database Path
  - Web Site
  - Database Name
9. Click the **File** menu, and then click **Save Application.Class.mpx**.
10. In Solution Explorer, right-click the **Classes** folder, click **Add**, and then click **New Item**.
11. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Class**.
12. In the **Name** box, remove the existing text, type **DistributedApplication.Class.mpx**, and then click **Add**.
13. In the line that begins with **ClassType ID="CONTOSO.DinnerNow.DistributedApplication"**, change the **Base** element to "**System!System.Service**".
14. Change the **Singleton** element to "true".
15. In the line that begins with <Name>**DistributedApplication Class**</Name>, change **DistributedApplication Class** to **DinnerNow**.
16. Click the **File** menu, and then click **Save DistributedApplication.Class.mpx**.

► **Task 3: Define relationships between the application and application components**

1. Right-click the **Classes** folder, click **Add**, then click **New Item**.
2. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Relationship**.
3. In the **Name** box, remove the existing text and type **DaContainsApp.Relationship.mpx**, and then click **Add**.
4. Change the line that reads <Source ID="Source" Type="" /> to <Source ID="Source" Type="CONTOSO.DinnerNow.DistributedApplication" />.
5. Change the line that reads <Target ID="Target" Type="" /> to <Target ID="Target" Type="CONTOSO.DinnerNow.Application" />.

6. In the line that begins <Name>**DaContainsApp Relationship**</Name>, change the **DaContainsApp Relationship** to **DinnerNow Distributed Application Contains Application**.
7. Click the **File** menu, and then click **Save DaContainsApp.Relationship.mpx**.
8. Right-click the **Classes** folder, click **Add**, and then click **New Item**.
9. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Relationship**.
10. In the **Name** box, remove the existing text and type **AppContainsWebSite.Relationship.mpx**, and then click **Add**.
11. Change the line <Source ID="Source" Type="" /> to <Source ID="Source" Type="CONTOSO.DinnerNow. Application"/>.
12. Change the line <Target ID="Target" Type="" /> to <Target ID="Target" Type="IIS2008!Microsoft.Windows.InternetInformationServices.2008.WebSite"/>.
13. In the line that reads <Name>**AppContainsWebSite Relationship** </Name>, change **AppContainsWebSite Relationship** to **DinnerNow Application Contains Web Site**.
14. Click the **File** menu, and then click **Save AppContainsWebSite.Relationship.mpx**.
15. Right-click the **Classes** folder, click **Add**, and then click **New Item**.
16. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Relationship**.
17. In the **Name** box, remove the existing text and type **AppContainsDB.Relationship.mpx**, and then click **Add**.
18. Change the line <Source ID="Source" Type="" /> to <Source ID="Source" Type="CONTOSO.DinnerNow. Application"/>.
19. Change the line <Target ID="Target" Type="" /> to <Target ID="Target" Type="SQL!Microsoft.SQLServer.Database"/>.
20. In the line that reads <Name>**AppContainsDB Relationship**</Name>, change **AppContainsDB Relationship** to **DinnerNow Application Contains Database**.
21. Click the **File** menu, and then click **Save AppContainsDB.Relationship.mpx**
22. Click the **BUILD** menu and then click **Build Solution**.
23. In the **Output** window wait until the build process completes. You should see a **Build 1 succeeded** message appear. If there are any filed or warning messages you must correct these before moving on through the lab. Errors and Warnings are most likely due to incorrect case when creating the classes and modifying elements within a class. For example, when creating the project at the beginning of the lab if you entered **Contoso.DinnerNow** as the Solution name instead of **CONTOSO.DinnerNow** this would cause the build process to fail.

#### ► Task 4: Create the health model

1. Right-click the **Discoveries** folder, click **Add**, and then click **New Item**.
2. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Discovery**.
3. In the **Name** box, remove the existing text, type **Discoveries.mptg**, and then click **Add**.
4. In the **Discoveries.mptg** window that opens, click **NewDiscovery**.
5. From the **Properties** window, configure the following properties:
  - a. Description: **Seed discovery for DinnerNow Application**
  - b. Display Name: **DinnerNow Application Discovery (Filtered Registry)**

- c. ID: **CONTOSO.DinnerNow.Application.Discovery.FilteredRegistry**
- d. Target: Click the (...) button and in the Choose a Class window that opens click **Microsoft.Windows.Server.Computer** and then click **OK**.
- e. Next to the **Discovery Classes** box, click (...).
- f. In the **Discovery Classes Collection Editor** window that opens, click **Add**.
- g. Next to the **Class** box, click (...).
- h. In the **Choose a Class** window that opens, click **CONTOSO.DinnerNow.Application**, and then click **OK**.
- i. To close the **Discovery Classes Collection Editor** window, click **OK**.
- j. Next to the **Data Source Type ID** box, click (...).
- k. In the **Choose a Data Source Module Type** window that opens, click **Microsoft.Windows.FilteredRegistryDiscoveryProvider**, and then click **OK**.
- l. Next to the **Data Source Configuration** box, click (...).
- m. Add the following XML code between the **Configuration** tags, and then click **OK**.

```

<ComputerName>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/NetworkName
$</ComputerName>
 <RegistryAttributeDefinitions>
 <RegistryAttributeDefinition>
 <AttributeName>Installed</AttributeName>
 <Path>SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\><Path>
 <PathType>1</PathType>
 <AttributeType>0</AttributeType>
 </RegistryAttributeDefinition>
 <RegistryAttributeDefinition>
 <AttributeName>InstallPath</AttributeName>
 <Path>SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\><Path>
 <PathType>1</PathType>
 <AttributeType>1</AttributeType>
 </RegistryAttributeDefinition>
 <RegistryAttributeDefinition>
 <AttributeName>DatabasePath</AttributeName>
 <Path>SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo\><Path>
 <PathType>1</PathType>
 <AttributeType>1</AttributeType>
 </RegistryAttributeDefinition>
 <RegistryAttributeDefinitions>
 <Frequency>60</Frequency>
 <ClassId>$MPElement[Name="CONTOSO.DinnerNow.Application"]$</ClassId>
 <InstanceSettings>
 <Settings>
 <Setting>
 <Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
 <Value>$Target/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Value>
 </Setting>
 <Setting>
 <Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/InstallPath$</Name>
 <Value>$Data/Values/InstallPath$</Value>
 </Setting>
 <Setting>
 <Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/DatabasePath$</Name>

```

```

 <Value>$Data/Values/DatabasePath$</Value>
 </Setting>
 <Setting>

<Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/Website$</Name>
 <Value>W3SVC/1</Value>
 </Setting>
 <Setting>

<Name>$MPElement[Name="CONTOSO.DinnerNow.Application"]/DatabaseName$</Name>
 <Value>DinnerNow</Value>
 </Setting>
 <Setting>
 <Name>$MPElement[Name="System!System.Entity"]/DisplayName$</Name>

<Value>$Target/Property[Type="System!System.Entity"]/DisplayName$</Value>
 </Setting>
 </Settings>
</InstanceSettings>
<Expression>
 <SimpleExpression>
 <ValueExpression>
 <XPathQuery Type="String">Values/Installed</XPathQuery>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">true</Value>
 </ValueExpression>
 </SimpleExpression>
</Expression>

```

- Click the **File** menu, and then click Save **Discoveries.mptg**.

► **Task 5: Create the relationship mapper module**

- Right-click the **Modules and Types** folder, click **Add**, and then click **New Item**.
- In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Empty Management Pack Fragment**.
- In the **Name** box, remove the existing text, type **FilteredRelationshipMapper.DataSource.mpx**, and then click **Add**.
- In the **FilteredRelationshipMapper.DataSource.mpx** window that opens, add the following XML code between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
<ModuleTypes>
 <DataSourceModuleType ID="CONTOSO.DinnerNow.FilteredRelationshipMapper"
Accessibility="Internal" Batching="false">
 <Configuration>
 <IncludeSchemaTypes>
 <SchemaType>System!System.Discovery.MapperSchema</SchemaType>
 </IncludeSchemaTypes>
 <xsd:element minOccurs="1" name="Interval" type="xsd:integer" />
 <xsd:element minOccurs="0" name="SyncTime" type="xsd:string" />
 <xsd:element minOccurs="1" name="PropertyName" type="xsd:string" />
 <xsd:element minOccurs="1" name="PropertyValue" type="xsd:string" />
 <xsd:element minOccurs="1" name="RelationshipId" type="xsd:string" />
 <xsd:element minOccurs="0" name="SourceTypeId" type="xsd:string" />
 <xsd:element minOccurs="0" name="TargetTypeId" type="xsd:string" />
 <xsd:element minOccurs="1" name="SourceRoleSettings" type="SettingsType" />
 <xsd:element minOccurs="1" name="TargetRoleSettings" type="SettingsType" />
 </Configuration>
 <ModuleImplementation Isolation="Any">
 <Composite>

```

```

<MemberModules>
 <DataSource ID="Scheduler"TypeID="System!System.Discovery.Scheduler">
 <Scheduler>
 <SimpleRecurringSchedule>
 <Interval>$Config/Interval$</Interval>
 <SyncTime>$Config/SyncTime$</SyncTime>
 </SimpleRecurringSchedule>
 <ExcludeDates />
 </Scheduler>
 </DataSource>
 <ConditionDetection ID="Filter"
 TypeID="System!System.ExpressionFilter">
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <Value Type="String">$Config/PropertyName$</Value>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">$Config/PropertyValue$</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>
 </ConditionDetection>
 <ConditionDetection ID="Mapper"
 TypeID="System!System.Discovery.RelationshipSnapshotDataMapper">
 <RelationshipId>$Config/RelationshipId$</RelationshipId>
 <SourceRoleSettings>$Config/SourceRoleSettings$</SourceRoleSettings>
 <TargetRoleSettings>$Config/TargetRoleSettings$</TargetRoleSettings>
 </ConditionDetection>
</MemberModules>
<Composition>
 <Node ID="Mapper">
 <Node ID="Filter">
 <Node ID="Scheduler" />
 </Node>
 </Node>
</Composition>
</Composite>
</ModuleImplementation>
<OutputType>System!System.Discovery.Data</OutputType>
</DataSourceModuleType>
</ModuleTypes>
</TypeDefinitions>

```

5. Click the **File** menu, and then click **Save FilteredRelationshipMapper.DataSource.mpx**.

► **Task 6: Define the health mode for the database discovery**

1. In Solution Explorer, expand the **Discoveries** folder, right-click **Discoveries.mptg**, and then click **Open**.
2. In the **Discoveries.mptg** window that opens, right-click in the white space area, and then click **Add Template**.
3. In the **Add Template** window that opens, click **Discovery (Custom)**, and then click **OK**.
4. Click **NewDiscovery** and, in the **Properties** pane, under the **General** section, configure the following properties:
  - a. Display Name: **DinnerNow Database Discovery (Filtered Relationship Map)**
  - b. ID: **Database.Discovery.FilteredRelationshipMap**
  - c. Target: Click (...) and in the **Choose a Class** window that opens click **CONTOSO.DinnerNow.Application** and then click **OK**.

- d. Next to the **Discovery Relationships** box, click (...).
- e. In the **Discovery Relationships Collection Editor** window that opens, click **Add**.
- f. Next to the **Relationship** box, click (...).
- g. In the **Choose a Relationship** window that opens, click **CONTOSO.DinnerNow.AppContainsDB**, and then click **OK**.
- h. In the **Discovery Relationships Collection Editor** window, click **OK**.
- i. Next to the **Data Source Type ID** box, click (...).
- j. In the **Choose a Data Source Module Type** window that opens, click **CONTOSO.DinnerNow.FileteredRelationshipMapper**, and then click **OK**.
- k. Next to the **Data Source Configuration** box, click (...).
- l. Add the following XML code between the **Configuration** tags, and then click **OK**.

```

<Interval>60</Interval>
<PropertyName>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/DatabaseName$</P
ropertyName>

<PropertyValue>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/DatabaseName$</
PropertyValue>
<RelationshipId>$MPElement[Name="CONTOSO.DinnerNow.AppContainsDB"]$</RelationshipId>
 <SourceRoleSettings>
 <Settings>
 <Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>

<Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
 </Setting>
 <Settings>
 </SourceRoleSettings>
 <TargetRoleSettings>
 <Settings>
 <Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>

<Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
 </Setting>
 <Setting>

<Name>$MPElement[Name="SQL!Microsoft.SQLServer.ServerRole"]/InstanceName$</Name>
 <Value>MSSQLSERVER</Value>
 </Setting>
 <Setting>

<Name>$MPElement[Name="SQL!Microsoft.SQLServer.Database"]/DatabaseName$</Name>

<Value>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/DatabaseName$</Value>
 </Setting>
 <Settings>
 </TargetRoleSettings>

```

5. Click the **File** menu, and then click **Save Discoveries.mptg**.

#### ► Task 7: Define the health model for the website discovery

1. In Solution Explorer, expand the **Discoveries** folder, right click **Discoveries.mptg**, and then click **Open**.

2. In the **Discoveries.mptg** window that opens, right-click in the white space area, and then click **Add Template**.
  3. In the **Add Template** window that opens, click **Discovery (Custom)**, and then click **OK**.
  4. Click **NewDiscovery**, and in the **Properties** pane, under the **General** section, configure the following properties :
    - a. Display Name: **DinnerNow Web Site Discovery (Filtered Relationship Map)**
    - b. ID: **WebSite.Discovery.FilteredRelationshipMap**
    - c. Target: Click (...) and in the **Choose a Class** window click **CONTOSO.DinnerNow.Application** and then click **OK**.
    - d. Next to the **Discovery Relationships** box, click (...).
    - e. In the **Discovery Relationships Collection Editor** window that opens, click **Add**.
    - f. Next to the **Relationship** box, click (...).
    - g. In the **Choose a Relationship** window that opens, click **CONTOSO.DinnerNow.AppContainsWebSite**, and then click **OK**.
    - h. In the **Discovery Relationships Collection Editor** window, click **OK**.
    - i. Next to the **Data Source Type ID** box, click (...).
    - j. In the **Choose a Data Source Module Type** window that opens, click **CONTOSO.DinnerNow.FileteredRelationshipMapper**, and then click **OK**.
    - k. Next to the **Data Source Configuration** box, click (...).
    - l. Add the following XML code between the **Configuration** tags.

```
<Interval>60</Interval>
<PropertyName>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website$</Proper
tyName>
<PropertyValue>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website$</Prope
rtyValue>
<RelationshipId>$MPElement[Name="CONTOSO.DinnerNow.AppContainsWebSite"]$</Relationshi
pId>
<SourceRoleSettings>
<Settings>
<Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
<Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
</Setting>
</Settings>
</SourceRoleSettings>
<TargetRoleSettings>
<Settings>
<Setting>

<Name>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Name>
<Value>$Target/Host/Property[Type="Windows!Microsoft.Windows.Computer"]/PrincipalName
$</Value>
</Setting>
<Setting>

<Name>$MPElement[Name="IIS!Microsoft.Windows.InternetInformationServices.WebSite"]/Si
teID$</Name>
<Value>$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website$</Value>
</Setting>
</Settings>
```

```
</TargetRoleSettings>
```

5. Find the line that displays  
**<Value>\$Target/Property[Type="CONTOSO.DinnerNow.Application"]/Website\$</Value>**  
which is the 5<sup>th</sup> line from the bottom.
6. Notice that the quotes at the end of the section "CONTOSO.DinnerNow.Application" are slightly different to the quotes at the beginning. You may need to paste this section into Notepad to see the difference. When you build the Management Pack later in this exercise if this is not fixed an error will be produced. The quotes at the end of the section are wrong.
7. To fix this copy the quotes at the beginning of the section as highlighted in yellow here:  
"CONTOSO.DinnerNow.Application" and then paste the quotes overwriting the quotes at the end of the section as highlighted here in yellow: "CONTOSO.DinnerNow.Application"
8. Click **OK** to close the **Enter Data Source Module Type configuration** window.
9. Click the **File** menu, and then click **Save Discoveries.mptg**.

► **Task 8: Define the health model for the distributed application discovery**

1. In Solution Explorer, expand the **Discoveries** folder, right click **Discoveries.mptg**, and then click **Open**.
2. In the **Discoveries.mptg** window that opens, right-click in the white space area, and then click **Add Template**.
3. In the **Add Template** window that opens, click **Discovery (Custom)**, and then click **OK**.
4. Click **NewDiscovery** and in the **Properties** pane, under the **General** section, configure the following properties:
  - a. Display Name: **DinnerNow Distributed Application Discovery (Group Populator)**
  - b. ID: **CONTOSO.DinnerNow.DistributedApplication.Discovery.GroupPopulator**
  - c. Target: Click (...) and in the Choose a Class window click  
**CONTOSO.DinnerNow.DistributedApplication** and then click **OK**.
  - d. Next to the **Discovery Relationships** box, click (...).
  - e. In the **Discovery Relationships Collection Editor** window that opens, click **Add**.
  - f. Next to the **Relationship** box, click (...).
  - g. In the **Choose a Relationship** window that opens, click  
**CONTOSO.DinnerNow.DaContainsApp**, and then click **OK**.
  - h. In the **Discovery Relationships Collection Editor** window, click **OK**.
  - i. Next to the **Data Source Type ID** box, click (...).
  - j. In the **Choose a Data Source Module Type** window that opens, click  
**Microsoft.SystemCenter.GroupPopulator**, and then click **OK**.
  - k. Next to the **Data Source Configuration** box, click (...).
  - l. Add the following XML code between the **Configuration** tags, and then click **OK**.

```
<RuleId>$MPElement$</RuleId>

<GroupInstanceId>$MPElement[Name="CONTOSO.DinnerNow.DistributedApplication"]$</GroupInstanceId>
 <MembershipRules>
 <MembershipRule>
```

```

<MonitoringClass>$MPElement [Name="CONTOSO.DinnerNow.Application"]$</MonitoringClass>
<RelationshipClass>$MPElement [Name="CONTOSO.DinnerNow.DaContainsApp"]$</RelationshipClass>
 </MembershipRule>
</MembershipRules>

```

5. Click the **File** menu, and then click **Save Discoveries.mptg**

► **Task 9: Define the health model dependency monitors**

1. In Solution Explorer, right-click the **Monitors** folder, click **Add**, and then click **New Item**.
2. In the **Add New Item – CONTOSO.DinnerNow** dialog box that opens, click **Monitor (dependency)**.
3. In the **Name** box, remove the existing text and type **Monitors.mptg**, and then click **Add**.
4. In the **Monitors.mptg** window that opens, click **NewDependencyMonitor**.
5. In the **Properties** pane, configure the General properties as follows:
  - a. Display Name: **DinnerNow Database Dependency Monitor**
  - b. ID: **Database.DependencyMonitor**
  - c. Target: Click (...) and in the **Choose a Class** window click **CONTOSO.DinnerNow.Application** and then click **OK**.
6. Configure the **Dependency Monitor** properties as follows:
  - a. Health Roll-up Algorithm: **WorstOf**
  - b. Relationship Type: Click (...) and in the **Choose a Relationship** window click **CONTOSO.DinnerNow.AppContainsDB** and then click **OK**.
  - c. Member Monitor: Click (...) and in the **Choose a Monitor** window click **System.Health.AvailabilityState** and then click **OK**.
  - d. Member Unavailable: **Roll up as error**
  - e. Parent Monitor ID: Click (...) and in the **Choose a Monitor** window click **System.Health.EntityState** and then click **OK**.
7. Click the **File** menu, and then click **Save Monitors.mptg**.
8. In the **Monitors.mptg** window, right-click in the white space area, and then click **Add Template**.
9. In the **Add Template** window that opens, click **Monitor (Dependency)**, and then click **OK**.
10. Click **NewDependencyMonitor**.
11. In the **Properties** pane, configure the **General** properties as follows:
  - a. Display Name: **DinnerNow Web Site Dependency Monitor**
  - b. ID: **WebSite.DependencyMonitor**
  - c. Target: Click (...) and in the **Choose a Class** window click **CONTOSO.DinnerNow.Application** and then click **OK**.
12. Configure the **Dependency Monitor** properties as follows:
  - a. Health Roll-up Algorithm: **WorstOf**
  - b. Relationship Type: Click (...) and in the Choose a Relationship window click **CONTOSO.DinnerNow.AppContainsWebSite** and then click **OK**.

- c. Member Monitor: Click (...) and in the Choose a Monitor window click **System.Health.AvailabilityState** and then click **OK**.
  - d. Member Unavailable: **Roll up as error**
  - e. Parent Monitor ID: Click (...) and in the Choose a Monitor window click **System.Health.EntityState** and then click **OK**.
13. Click the **File** menu, and then click **Save Monitors.mptg**.
14. In the **Monitors.mptg** window, right-click in the white space area, and then click **Add Template**.
15. In the **Add Template** window that opens, click **Monitor (Dependency)**, and then click **OK**.
16. Click **NewDependencyMonitor**.
17. In the **Properties** pane, configure the **General** properties as follows:
- a. Display Name: **DinnerNow Application Dependency Monitor**
  - b. ID: **Application.DependencyMonitor**
  - c. Target: Click (...) and in the **Choose a Class** window click **CONTOSO.DinnerNow.DistributedApplication** and then click **OK**.
  - d. Configure the **Dependency Monitor** properties as follows:
  - e. Health Roll-up Algorithm: **WorstOf**
  - f. Relationship Type: Click (...) and in the **Choose a Relationship** window click **CONTOSO.DinnerNow.DaContainsApp** and then click **OK**.
  - g. Member Monitor: Click (...) and in the **Choose a Monitor** window click **System.Health.AvailabilityState** and then click **OK**.
  - h. Member Unavailable: **Roll up as error**
  - i. Parent Monitor ID: Click (...) and in the Choose a Monitor window click **System.Health.EntityState** and then click **OK**.
18. Click the **File** menu, and then click **Save Monitors.mptg**.
- **Task 10: Define the URL probe composite data source**
1. In Solution Explorer, right-click the **Modules and Types** folder, click **Add**, then click **New Item**.
  2. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Empty Management Pack Fragment**.
  3. In the **Name** box, remove the existing text and type **UrlProbe.DataSource.mpx**, and then click **Add**.
  4. Add the following XML code between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
 <ModuleTypes>
 <DataSourceModuleType ID="CONTOSO.DinnerNow.URLProbe" Accessibility="Internal"
Batching="false">
 <Configuration>
 <xsd:element minOccurs="1" name="URL" type="xsd:string" />
 </Configuration>
 <ModuleImplementation Isolation="Any">
 <Composite>
 <MemberModules>
 <DataSource ID="Scheduler"TypeID="System!System.SimpleScheduler">
 <IntervalSeconds>60</IntervalSeconds>
 <SyncTime>00:00</SyncTime>
 </DataSource>
 </MemberModules>
 </Composite>
 </ModuleImplementation>
 </DataSourceModuleType>
 </ModuleTypes>
</TypeDefinitions>

```

```

<ProbeAction ID="PowerShell"
TypeID="Windows!Microsoft.Windows.PowerShellPropertyBagProbe">
 <ScriptName>CONTOSO.DinnerNow.URLProbe.ps1</ScriptName>
 <ScriptBody><![CDATA[
param($URL)
$req = [System.Net.HttpWebRequest]::Create($URL);
$req.Credentials = [System.Net.CredentialCache]::DefaultCredentials
$res = $req.GetResponse();
$api = New-Object -comObject 'MOM.ScriptAPI'
$bag = $api.CreatePropertyBag()
if ($res.StatusCode -eq 200){
 $bag.AddValue('Match', 'True')
} else{
 $bag.AddValue('Match', 'False')
}
$bag
]]></ScriptBody>
 <Parameters>
 <Parameter>
 <Name>URL</Name>
 <Value>$Config/URL$</Value>
 </Parameter>
 </Parameters>
 <TimeoutSeconds>30</TimeoutSeconds>
</ProbeAction>
</MemberModules>
<Composition>
 <Node ID="PowerShell">
 <Node ID="Scheduler" />
 </Node>
</Composition>
</Composite>
</ModuleImplementation>
<OutputType>System.PropertyBagData</OutputType>
</DataSourceModuleType>
</ModuleTypes>
<TypeDefinitions>

```

5. In the XML, replace the second <**TypeDefinitions**> line (which is located on the second to last line) and replace it with <**/TypeDefinitions**>
6. Click the **File** menu, and then click **Save UrlProbe.DataSource.mpx**.

► **Task 11: Define the custom URL probe monitor**

1. In Solution Explorer, right-click the **Modules and Types** folder and then click **Add** then click **New Item**.
2. In the **Add New Item – CONTOSO.DinnerNow** window that opens click **Empty Management Pack Fragment**.
3. In the **Name** box, remove the existing text and then type **URLProbe.MonitorType.mpx** and then click **Add**.
4. Add the following XML code between the **ManagementPackFragment** tags.

```

<TypeDefinitions>
 <MonitorTypes>
 <UnitMonitorType ID="CONTOSO.DinnerNow.URLProbe.MonitorType"
Accessibility="Internal">
 <MonitorTypeStates>
 <MonitorTypeState ID="DOWN" NoDetection="false" />
 <MonitorTypeState ID="UP" NoDetection="false" />
 </MonitorTypeStates>
 <Configuration>
 <xsd:element minOccurs="1" name="URL" type="xsd:string" />

```

```

</Configuration>
<MonitorImplementation>
 <MemberModules>
 <DataSource ID="URLPROBE" TypeID="CONTOSO.DinnerNow.URLProbe">
 <URL>$Config/URL$</URL>
 </DataSource>
 <ConditionDetection ID="CheckDOWN"
TypeID="System!System.ExpressionFilter">
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <XPathQuery Type="String">Property[@Name="Match"]</XPathQuery>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">False</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>
 </ConditionDetection>
 <ConditionDetection ID="CheckUP" TypeID="System!System.ExpressionFilter">
 <Expression>
 <SimpleExpression>
 <ValueExpression>
 <XPathQuery Type="String">Property[@Name="Match"]</XPathQuery>
 </ValueExpression>
 <Operator>Equal</Operator>
 <ValueExpression>
 <Value Type="String">True</Value>
 </ValueExpression>
 </SimpleExpression>
 </Expression>
 </ConditionDetection>
 </MemberModules>
 <RegularDetections>
 <RegularDetection MonitorTypeStateID="DOWN">
 <Node ID="CheckDOWN">
 <Node ID="URLPROBE" />
 </Node>
 </RegularDetection>
 <RegularDetection MonitorTypeStateID="UP">
 <Node ID="CheckUP">
 <Node ID="URLPROBE" />
 </Node>
 </RegularDetection>
 </RegularDetections>
</MonitorImplementation>
</UnitMonitorType>
</MonitorTypes>
</TypeDefinitions>

```

- Click the **File** menu, and then click **Save URLProbe.MonitorType.mpx**.

#### ► Task 12: Define the health model for the monitor

- In Solution Explorer, expand the **Monitors** folder, right-click **Monitors.mptg**, and then click **Open**.
- In the **Monitors.mptg** window that opens, right-click in the white space area, and then click **Add Template**.
- In the **Add Template** window that opens, click **Monitor (Unit)**, and then click **OK**.
- Click **NewUnitMonitor**.
- In the **Properties** window, configure the **General** properties as follows:
  - Display Name: **DinnerNow Website URL Probe Monitor**

- ID: **Website.UrlProbeMonitor**
  - Target: Click (...) and in the Choose a Class window click **CONTOSO.DinnerNow.Application** and then click **OK**.
6. Configure the **Unit Monitor** properties as follows:
- a. Monitor Type ID: Click (...) and in the **Choose a Unit Monitor Type** window click **CONTOSO.DinnerNow.URLProbe.MonitorType** and then click **OK**.
  - b. Parent Monitor ID: Click (...) and in the **Choose a Monitor** window click **System.Health.AvailabilityState** and then click **OK**.
  - c. Next to the **Monitor Operational States** box, click (...).
  - d. In the **Map monitor conditions to health states** window that opens, click the **Health State** drop-down list for **UP**, click **Healthy**, and then click **OK**.
  - e. Next to the **Monitor Configuration** box, click (...).
  - f. In the **Enter Unit Monitor Type configuration** window that opens, between the **Configuration** tags, enter the following XML code, and then click **OK**.

```
<URL>http://localhost/DinnerNow/</URL>
```

7. Click the **File** menu, and then click **Save Monitors.mptg**.

► **Task 13: Define the health model for the rule**

1. In Solution Explorer, right-click the **Rules** folder, click **Add**, then click **New Item**.
2. In the **Add New Item – CONTOSO.DinnerNow** dialog box that opens, click **Snippet Template**.
3. In the **Name** box, remove the existing text and type **WindowsPerformanceCounters.templatesnippet**, and then click **Add**.
4. Replace the line that reads **<Name>Collection rule for performance counter #text('Perf Counter Name')#.</Name>** with **<Name>#text('Rule Id')# - Snippet Generated</Name>**.
5. Replace the text that reads **Target="#alias('Microsoft.Windows.Library')#!Microsoft.Windows.Computer"** with **Target="CONTOSO.DinnerNow.Application"**.
6. Replace the text that reads **<ComputerName>\$Target/Property[Type ...** with **<ComputerName>\$Target/Host/Property[Type ....**
7. Click the **File** menu, and then click **Save WindowsPerformanceCounters.templatesnippet**.
8. In Solution Explorer, right-click the **Rules** folder, click **Add**, then click **New Item**.
9. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Snippet Data**.
10. In the **Name** box, remove the existing text and type **WindowsPerformanceCounterRules.mpsd**, and then click **Add**.
11. In the **WindowsPerformanceRules.mpsd** window that opens, click **Select snippet type**.
12. In the **Select Snippet** window that opens, click **Rules\WindowsPerformanceCounters**, and then click **OK**.
13. Click the **Click here to add a new item** link.
14. Configure the following settings:
  - RuleID: **WPC.Process.WorkingSet.w3wp**

- Perf Counter Name: **Process**
  - Perf Object Name: **Working Set**
  - Perf Instance Name: **w3wp**
  - Collection Frequency: **900**
15. Click the **Click here to add a new item** link.
16. Configure the following settings:
- RuleID: **WPC.WebService.CurrentConnections.DefaultWebSite**
  - Perf Counter Name: **Web Service**
  - Perf Object Name: **Current Connections**
  - Perf Instance Name: **Default Web Site**
  - Collection Frequency: **900**
17. Click the **File** menu, and then click **Save WindowsPerformanceRules.mpsd**.
- **Task 14: Define the views in the Operations console**
1. In Solution Explorer, right-click the **Views** folder, click **Add**, then click **New Item**.
  2. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **Folder & Folder Item**.
  3. In the **Name** box, remove the existing text and type **Folder.mpx**, and then click **Add**.
  4. In the line that reads **<Name>Folder Folder</Name>**, replace **Folder Folder** with **\_CONTOSO.DinnerNow**.
  5. Click the **File** menu, and then click **Save Folder.mpx**.
  6. In Solution Explorer, right-click the **Views** folder, click **Add**, then click **New Item**.
  7. In the **Add New Item – CONTOSO.DinnerNow** window that opens, click **View (Custom)**.
  8. In the name box, remove the existing text and type **Views.mptg**, and then click **Add**.
  9. In the **Views.mptg** window that opens click **NewView**.
  10. In the **Properties** window, configure the **General** properties as follows:
    - Display Name: **Application State**
    - ID: **ApplicationStateView**
    - Target: Click (...) and in the **Choose a Class** window that opens click **CONTOSO.DinnerNow.Application** and then click **OK**.
  11. Configure the View properties as follows:
    - View Folder: Click (...) and in the **Choose a Folder** window click **Contoso.DinnerNow.Folder** and then click **OK**.
    - View Type ID: Click (...) and in the **Choose a View Type** window click **Microsoft.SystemCenter.StateViewType** and then click **OK**.
  12. Click the **File** menu, and then click **Save Views.mptg**
  13. Right-click in the white area of the **Views.mptg** window, and then click **Add Template**.
  14. In the **Add Template** window that opens, click **View (Custom)**, and then click **OK**.
  15. Click **NewView**, and then in the **Properties** pane, configure the **General** properties as follows:

- Display Name: **DinnerNow Distributed Application Diagram**
  - ID: **DistributedApplicationDiagram**
  - Target: Click (...) and in the **Choose a Class** window click **CONTOSO.DinnerNow.DistributedApplication** and then click **OK**.
16. Configure the View properties as follows:
- View Folder: Click (...) and in the **Choose a Folder** window click **Contoso.DinnerNow.Folder** and then click **OK**.
  - View Type ID: Click (...) and in the **Choose a View Type** window click **Microsoft.SystemCenter.DiagramViewType** and then click **OK**.
17. Click the **File** menu, and then click **Save Views.mptg**.
- **Task 15: Build and import the Management Pack**
1. Click the **File** menu, and then click **Save All**.
  2. Click the **Build** menu, and then click **Build Solution**.
  3. Wait for the build to complete, and then exit Microsoft Visual Studio.
  4. On LON-MS1, open the Operations console.
  5. Click the **Administration** pane, and then click **Management Packs**.
  6. From the **Tasks** pane, click **Import Management Packs**.
  7. In the **Import Management Packs** window that opens, click **Add**, and then click **Add from disk**.
  8. In the **Online Catalog Connection** window that opens, click **No**.
  9. In the **Select Management Pack to import** window that opens, in the **File name** box, type **\LON-AP1\C\$**, and then press Enter on the keyboard.
  10. Expand **Temp\DinnerNow\2012TMP\CONTOSO.DinnerNow\CONTOSO.DinnerNow\bin\Debug**, click **CONTOSO.DinnerNow.xml**, and then click **Open**.
  11. Click **Install**.
  12. Wait for the Management Pack import to complete, and then click **Close**.
  13. Click the **Monitoring** pane, expand the **\_CONTOSO.DinnerNow** folder, and then click the **Application State** view.
  14. Wait for the **DinnerNow** application to be discovered and shown in a healthy state. This can take up to 10 minutes.
  15. Click the **DinnerNow Distributed Application** view and expand the components groups to review the application components that have been discovered.

**Results:** After this exercise, you should have created a Management Pack by using VSAE. Included in the Management Pack should be various discoveries, rules, monitors, and views that are used to discover and monitor the DinnerNow application that is running on LON-AP2. After you import the Management Pack, you should be able to confirm that the DinnerNow application is discovered and is displayed in a healthy state.

## Exercise 3: Alternative to Exercise 2

### ► Task 1: Open the Visual Studio DinnerNow project

1. Logon to LON-AP1, click **Start** and then type **Visual Studio** then click **Visual Studio Tools**.
2. In the **Shortcuts** window that opens double-click **VS2013 x64 Native Tools Command Prompt**.
3. In the **Administrator: VS2013 x64 Native Tools Command Prompt** window that opens type the following and then press enter on the keyboard:

```
CD "C:\Program Files (x86)\Microsoft Visual Studio
12.0\Common7\IDE\CommonExtensions\Microsoft\Editor"
```

4. Type the following command and then press enter on the keyboard:

```
gacutil /i Microsoft.VisualStudio.Text.Logic.dll
```

5. Close the **Administrator: VS2013 x64 Native Tools Command Prompt** window.
6. From the desktop double-click **Visual Studio 2013**.
7. In **Visual Studio**, click the **File** menu, click **Open**, and then click **Project\Solution**.
8. In the **Open Project** window that opens browse to **C:\Module 9\Contoso.DinnerNow** then click **Contoso.DinnerNow** where the **Type** column displays **Microsoft Visual Studio Solution** and then click **Open**.

### ► Task 2: Build and import the Management Pack

1. Click the **File** menu, and then click **Save All**.
2. Click the **Build** menu, and then click **Build Solution**.
3. Wait for the build to complete, and then exit Microsoft Visual Studio.
4. On LON-MS1, open the Operations console.
5. Click the **Administration** pane, and then click **Management Packs**.
6. From the **Tasks** pane, click **Import Management Packs**.
7. In the **Import Management Packs** window that opens, click **Add**, and then click **Add from disk**.
8. In the **Online Catalog Connection** window that opens, click **No**.
9. In the **Select Management Pack to import** window that opens, in the **File name** box, type **\LON-AP1\C\$**, and then press Enter on the keyboard.
10. Expand **Module 9\CONTOSO.DinnerNow\CONTOSO.DinnerNow\bin\Debug**, click **CONTOSO.DinnerNow.xml**, and then click **Open**.
11. Click **Install**.
12. Wait for the Management Pack import to complete, and then click **Close**.
13. Click the **Monitoring** pane, expand the **\_CONTOSO.DinnerNow** folder, and then click the **Application State** view.
14. Wait for the **LON-AP2.CONTOSO.COM** computer to be discovered and shown in a healthy state. This can take up to 10 minutes.
15. Click **LON-AP2.CONTOSO.COM** and then in the **Detail View** pane, review the **DinnerNow** application details such as the **Database Path**, **Web Site** and **Database Name**.

16. Click the **DinnerNow Distributed Application Diagram** view and expand the components groups to review the application components that have been discovered.

**Results:** After this exercise you should have loaded the Visual Studio project into Visual Studio 2013 and then built the DinnerNow Management Pack. You should then have imported the Management Pack into Operations Manager and confirmed that the DinnerNow application is being monitored.

## Module 10: Integrating Operations Manager with Other System Center Components

# Lab: Configuring System Center Integration

### Exercise 1: Configure Service Manager Integration with Operations Manager

#### ► Task 1: Create the Operations Manager connector in Service Manager

1. Log on to LON-SM1, then from the **Desktop** double-click **Service Manager Console**.
2. In the Service Manager console, click the **Administration** pane, and then click **Connectors**.
3. From the **Tasks** pane, click **Create connector**, and then click **Operations Manager Alert connector**.
4. In the Operations Manager Alert Connector wizard, on the **Before You Begin** page, click **Next**.
5. On the **General** page, in the **Name** box, type **Operations Manager Alerts**, and then click **Next**.
6. On the **Server Details** page, in the **Server name** box, type **LON-MS1**, and then click **Next**.
7. In the **Credentials** dialog box that opens, in the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
8. On the **Alert Routing Rules** page, click **Next**.
9. On the **Schedule** page, click **Next**.
10. On the **Summary** page, click **Create**.
11. On the **Completion** page, click **Close**.

#### ► Task 2: Configure the Connector in Operations Manager

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Administration** pane, expand **Product Connectors**, and then click **Internal Connectors**.
3. In the **Details** pane, click **Alert Sync:Operations Manager Alerts**, and then from the **Tasks** pane, click **Properties**.

 **Note:** It might take five minutes for the **Alert Sync: Operations Manager Alerts** connector to appear.

 **Note:** If, after 10 minutes the **Alert Sync: Operations Manager Alerts** connector does not appear perform the following steps:

- a. Shutdown LON-MS1, LON-SM1 and LON-SQ1.
  - b. Start LON-SQ1 and wait until the login prompt appears.
  - c. Start LON-MS1 and wait until the login prompt appears.
  - d. Start LON-SM1 and wait until the login prompt appears.
  - e. After 5 minutes the **Alert Sync: Operations Manager Alerts** connector should appear. If it does not, delete the connector in Service Manager and then restart this exercise from Task 1.
4. In the **Alert Sync:Operations Manager Alerts – Product Connector Properties** window that opens, click **Add**.

5. In the **Product Connector Subscription Wizard** that starts, on the **General Properties** page, in the **Subscription** name box, type **Critical Alerts**, and then click **Next**.
6. On the **Groups** page, click **Next**.
7. On the **Targets** page, click **Next**.
8. On the **Criteria** page, click **Create**.
9. In the **Alert Sync:Operations Manager Alerts – Product Connector Properties** window, click **OK**.

► **Task 3: Generate an alert and confirm that an incident is created in Service Manager**

1. Log on to LON-MS1, and from **Services**, stop the **World Wide Web Publishing Service**.
  2. In the Operations console, click the **Monitoring** pane.
  3. Click **Active Alerts**.
  4. Wait for the **IIS 8 Web Site is unavailable** alert to be generated.
  5. Double-click the alert to open the **Alert Properties** window.
  6. In the **Alert Properties** window, note the **Ticket ID**.
  7. Close the **Alert Properties** window.
-  **Note:** It might take five minutes for the **Ticket ID** to be populated.
8. Log on to LON-SM1, and then open the **Service Manager console**.
  9. Click the **Work Items** pane, expand **Incident Management**, and then click **All Incidents**.
  10. Click the **ID** column to sort the view by ID.
  11. Double-click the incident with the **Ticket ID** that was noted in step 6.
  12. View the incident properties that were automatically configured by the Operations Manager Alert connector, such as **Description** and **Affected items**.
  13. On the incident form, click **Cancel**, and then click **Yes**.
  14. Click the **Configuration Items** pane, expand **Computers**, and then click **All Windows Computers**.
  15. From the **Details** pane, click **LON-MS1.CONTOSO.COM**, and then from the **Tasks** pane, click **Edit**.
  16. In the **Computer – LON-MS1.CONTOSO.COM** window that opens, click the **Related Items** tab.
  17. View the incidents that have automatically been added to the work items affecting this configuration items section.
  18. Close the **Computer – LON-MS1.CONTOSO.COM** window.
  19. In the **Service Manager** window that opens, click **Yes**.
  20. On LON-MS1, start the World **Wide Web Publishing Service**.
  21. Leave the connection to LON-MS1 open.

**Results:** After this exercise, you should have configured the Operations Manager Alert connector in Service Manager and Operations Manager. You should have also tested that the connector works as expected by generating an alert in Operations Manager, and then confirmed that an incident is automatically created in Service Manager. Finally, you should have viewed how Service Manager automatically updates the configuration items with related incidents when they are created in Service Manager.

## Exercise 2: Configure Operations Manager integration with Data Protection Manager

### ► Task 1: Import the DPM Management Packs

1. On LON-MS1, browse to **\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM\Management Packs\en-US**, and then copy both Management Packs to the LON-MS1 desktop.
2. Open the Operations console, and then click the **Administration** pane.
3. Click **Management Packs**, and then from the **Tasks** pane, click **Import Management Packs**.
4. In the **Import Management Packs** window that opens, click **Add**, then click **Add from disk**.
5. In the **Online Catalog Connection** dialog box, click **No**.
6. In the **Select Management Packs to import** window that opens click **Desktop**.
7. Multiselect **Microsoft.SystemCenter.DataProtectionManager.2012.Discovery.mp** and **Microsoft.SystemCenter.DataProtectionManager.2012.Library.mp**, and then click **Open**.
8. In the **Import Management Packs** window, click **Install**.
9. In the **Operations Manager** dialog box, click **Yes**.
10. Wait for the Management Packs to import, and then click **Close**.
11. Close the Operations console.

### ► Task 2: Install the DPM Central Console

1. Log on to LON-MS1 and close the **Operations console** if it is open.
2. Browse to **\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM\Redist\vcredist**, and then double-click **vcredist2008\_x64.exe**.
3. In the Microsoft Visual C ++ 2008 Redistributable Setup window that opens click Next.
4. On the License Terms page select I have read and accept the license terms and then click Install.
5. On the **Setup Complete** page click **Finish**.
6. Browse to **\LON-DC1\Media\System Center 2012 R2\Data Protection Manager\SCDPM**, and then double-click **Setup**.
7. In the **Data Protection Manager** window that opens, click **DPM Central Console**.
8. In the **Microsoft Software License Terms** window that opens, select **I accept the license terms and conditions**, and then click **OK**.
9. In the Data Protection Manager Central Console Setup wizard that starts, on the **Welcome** page, click **Next**.
10. On the **Central Console Opt-In** page, click **Next**.
11. On the **Prerequisites check** page, click **Next**.
12. On the **Installation settings** page, click **Next**.
13. On the **Microsoft Update Opt-In** page, select **I do not want to use Microsoft Update**, and then click **Install**.
14. In the **Data Protection Manager** window that opens, click **OK**.
15. When the installation has completed, click **Close**.

► **Task 3: Protect the Service Manager database**

1. Log on to LON-MS1, and from the desktop, double-click **Microsoft System Center Data Protection Manager**.
2. In the **Connect to DPM Server** window that opens, in the **DPM Server Name** box, type **LON-SC1.CONTOSO.COM**, and then click **OK**.
3. In the System Center 2012 DPM Administration Console that opens, click the **Management** pane.
4. On the ribbon, in the **Agents** group, click **Install**.
5. In the Protection Agents Installation Wizard that starts, on the **Select agent deployment method** page, select **Install agents**, and then click **Next**.
6. On the **Select computers** page, click **LON-SM1**, and then click **Add**.
7. If a **Microsoft System Center 2012 Data Protection Manager** dialog box appears, click **Yes**.
8. On the **Select computers** page, click **Next**.
9. On the **Enter credentials** page, in the **User name** box, type **Administrator**.
10. In the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
11. On the **Choose restart method** page, select **Yes, restart the selected computers after installing the protection agents (if required)**, and then click **Next**.
12. On the **Summary** page, click **Install**.
13. Wait for the installation to complete, and then click **Close**.
14. Leave the System Center 2012 DPM Administration Console open.
15. Log on to LON-SM1, click **Start**, type **SQL Server** and then click **SQL Server Management Studio**.
16. In the **Connect to Server** window that opens, in the **Server Type** box, make sure that **Database Engine** is displayed, and then click **Connect**.
17. In **SQL Server Management Studio**, expand **Security**, expand **Server Roles**, right-click **sysadmin**, and then click **Properties**.
18. In the **Server Roles Properties – sysadmin** window that opens, click **Add**.
19. In the **Select Server Login or Role** window that opens, click **Browse**.
20. In the **Browse for Objects** window that opens, select the check box next to **[NT AUTHORITY\SYSTEM]**, and then click **OK**.
21. In the **Select Server Login or Role** window, click **OK**.
22. In the **Server Role Properties - sysadmin** window, click **OK**.
23. Close **SQL Server Management Studio**, and then log off LON-SM1.
24. On LON-MS1, in the System Center 2012 DPM Administration Console, click the **Protection** pane, and then on the ribbon, in the **Protection** group, click **New**.
25. In the Create New Protection Group Wizard, on the **Welcome** page, click **Next**.
26. On the **Select protection group type** page, click **Next**.
27. On the **Select group members** page, expand **LON-SM1**, and then expand **All SQL Servers**.
28. Expand **LON-SM1**, select the check box next to **Service Manager**, and then click **Next**.
29. On the **Select data protection method** page, in the **Protection group name** box, type **SQL Server Databases**, and then click **Next**.

30. On the **Select short term goals** page, click **Next**.
31. On the **Review disk allocation page**, click **Next**.
32. On the **Choose replica creation method** page, click **Next**.
33. On the **Choose consistency check options** page, click **Next**.
34. On the **Summary** page, click **Create Group**.
35. On the **Status** page, monitor the **Results** column until both tasks display **Success**, and then click **Close**.
36. From the details pane, for the **ServiceManager** database, monitor the **Protection Status** column until the **Protection Status** changes from **Replica creation in progress** to **OK**. This confirms that that the **ServiceManager** database is now protected by DPM.
37. Close the DPM Administration Console.  
► **Task 4: Verify the protected data in Operations Manager**
  1. Log on to LON-MS1, and then open the Operations console.
  2. Click the **Monitoring** pane, and then expand **System Center 2012 R2 Data Protection Manager**.
  3. Expand **State views**, click **DPM Servers**, and then in the **Details** pane, click **LON-SC1**.
  4. Note the **DPM Server Tasks** that are available in the **Tasks** pane.
  5. Under **State Views**, click the other state views that are available, and then view the data that is shown in the **Details** pane.

Some views do not display any data at first, because the relevant discoveries have not yet run on the DPM Server. It is recommended that you revisit this section at the end of this lab and view the data that was collected by Operations Manager.

**Results:** After this exercise, you should have configured Operations Manager integration with Data Protection Manager by installing the DPM Central Console. You should have also used the DPM Administration Console from the Operations Manager server to install a protection agent on LON-SM1 and protect the Service Manager database.

## Exercise 3: Configure Orchestrator integration

### ► Task 1: Register and deploy Orchestrator Integration Packs

1. Log on to LON-SC1, click **Start**, type **Deployment Manager** and then click **Deployment Manager**.
2. In **System Center 2012 R2 Orchestrator Deployment Manager**, expand **Orchestrator Management Server**, right-click **Integration Packs**, and then click **Register IP with the Orchestrator Management Server**.
3. In the Integration Packs Registration wizard, on the **Welcome to the Integration Pack Registration Wizard** page, click **Next**.
4. On the **Select Integration Packs or Hotfixes** page, click **Add**.
5. In the **Open** box, type **\LON-DC1\Media**; in the **File name** box, click and then press Enter.
6. Open the **System Center 2012 R2** folder, and then open the **Orchestrator** folder.
7. Open the **Integration Packs** folder, click the **SC2012\_Operations\_Manager\_Integration\_Pack.oip** file, and then click **Open**.
8. Click **Add**, click **SC2012\_Service\_Manager\_Integration\_Pack.oip**, and then click **Open**.
9. On the **Select Integration Packs or Hotfixes** page, click **Next**.
10. On the **Completing the Integration Pack** wizard page, click **Finish**.
11. In the **Microsoft Software License Terms** window that opens, click **Accept**.
12. In the **Microsoft Software License Terms** window that opens, click **Accept**.
13. Right-click **Integration Packs**, and then click **Deploy IP to Runbook Server or Runbook Designer**.
14. In the Integration Pack Deployment Wizard that starts, on the **Welcome to the Integration Pack Deployment** wizard page, click **Next**.
15. On the **Deploy Integration Packs or Hotfixes** page, select all Integration Packs, and then click **Next**.
16. On the **Computer Selection Details** page, in the **Computer** box type **LON-SC1**, click **Add**, and then click **Next**.
17. On the **Installation Configuration** page, click **Next**.
18. On the **Completing the Integration Pack Deployment** wizard page, click **Finish**.
19. When the Integration Pack deployment has completed, close **System Center 2012 R2 Orchestrator Deployment Manager**.

### ► Task 2: Configure Orchestrator integration with Operations Manager and Service Manager

1. Log on to LON-SC1 and from the desktop double-click **Runbook Designer**.
2. In **System Center 2012 R2 Orchestrator Runbook Designer**, click **Options**, and then click **SC 2012 Operations Manager**.
3. In the **SC 2012 Operations Manager** window that opens, click **Add**.
4. In the **MS System Center Operations Manager Connection Settings** window that opens, in the **Name** box, type **LON-MS1**.
5. In the **Domain** box, type **CONTOSO**; in the **User name** box, type **Administrator**; and in the **Password** box, type **Pa\$\$w0rd**.
6. Click **Test Connection**.

7. In the **Success** window that opens, click **OK**, and then in the **MS System Center Operations Manager Connection Settings** window, click **OK**.
8. In the **SC 2012 Operations Manager** window, click **Finish**
9. From the **Options** menu click **SC 2012 Service Manager**.
10. In the **SC 2012 Service Manager** window that opens click **Add**.
11. In the **Connection** window that opens type **LON-SM1** in the **Name** and **Server** boxes.
12. Type **Contoso** in the **Domain** box and then type **Administrator** in the **User name** box.
13. Type **Pa\$\$w0rd** in the **Password** box and then click **Test Connection**.
14. In the **Connection** window that opens click **OK**.
15. Click **OK** on the **Connection** window and then click **Finish** on the **SC 2012 Service Manager** window.
16. Close the **Runbook Designer**.

**Results:** After this exercise, you should have configured Orchestrator integration with both Service Manager and Operations Manager. This included registering and deploying Orchestrator Integration Packs, installing the Operations Manager Console on the Orchestrator server, and then configuring the Orchestrator connections in the Runbook Designer.

## Exercise 4: Implementing Automatic Website Restart and Creating an Incident if it Fails

### ► Task 1: Configure Windows PowerShell for remote operations

1. Log on to LON-SC1, click **Start**, and then click **Windows PowerShell**.
2. In the **Administrator: Windows PowerShell** window that opens, type the following command, and then press Enter.

```
Set-ExecutionPolicy unrestricted
```

3. At the **Execution Policy Change** prompt, type **Y**, and then press Enter.
4. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter.

```
Enable-psremoting -force
```

5. Close the **Administrator: Windows PowerShell** window.
6. Repeat steps 1 through 5, and replace **LON-SC1** with **LON-MS1**.
7. Log on to LON-MS1, and then open **Server Manager**.
8. In **Server Manager**, click **Tools**, and then click **Computer Management**.
9. In Computer Management, expand **Local Users and Groups**, and then click **Groups**.
10. From the **Details** pane, right-click **Administrators**, and then click **Properties**.
11. In the **Administrators Properties** window that opens, click **Add**.
12. In the **Select Users, Computers, Service Accounts, or Groups** window that opens, in the box, type **Orchestrator\_SVC**, and then click **Check Names**.
13. In the **Select Users, Computers, Service Accounts, or Groups** window, click **OK**.
14. In the **Administrators Properties** window, click **OK**.
15. Close Computer Management, and then log off LON-MS1.

### ► Task 2: Import the runbook into Orchestrator

1. Log on to LON-SC1, and open **Windows Services**.
2. Ensure that the **Orchestrator Runbook Service** is running, if not, start it.
3. Open the **Runbook Designer** from the desktop.
4. In the Runbook Designer, expand **LON-SC1**, right-click **Runbooks**, and then click **Import**.
5. In the **Import** window that opens, click the **ellipsis** button (...); in the **Open** window, browse to drive **C:** click **Restart\_Website.ois\_export**; and then click **Open**.
6. In the **Import** window, in the **Password** box, type **Pa\$\$w0rd**, and then click **Finish**.
7. In the **Import/Export** window, click **OK**.
8. Expand **Runbooks**, and then click **Restart Web Site**.
9. From the toolbar, click **Run**.

► **Task 3: Stop the Default Web Site on LON-MS1 and confirm that runbook automatically restarts it**

1. Log on to LON-MS1, and then open the Operations console.
2. Click the **Monitoring** pane, and then click **Active Alerts**.
3. Click **Start**, and then click **Administrative Tools** and then double-click **Internet Information Services (IIS) Manager**.
4. Expand LON-MS1, and in the **Internet Information Services (IIS) Manager** window that opens, click **No**.
5. Expand **Sites**, and then click **Default Web Site**.
6. From the **Actions** pane, click **Stop** to stop the **Default Web Site**.
7. Close Internet Information Services (IIS) Manager.
8. Monitor the **Active Alerts** view in the Operations console, and then wait for the **IIS 8 Web Site is unavailable** alert to be generated.

 **Note:** After approximately two minutes, the alert disappears because Orchestrator has restarted the website. Operation Manager detects this and then automatically resolves the alert because the condition no longer exists. You may need to refresh the Active Alerts view.

9. Click **Start**, and then click **Administrative Tools** and then double-click **Internet Information Services (IIS) Manager**.
10. Expand LON-MS1, and in the **Internet Information Services (IIS) Manager** window that opens, click **No**.
11. Expand **Sites**, and then click **Default Web Site**.
12. Confirm that the **Default Web Site** is now running because the **Start** action is no longer available.

You might have to update the view to update the Actions list.

► **Task 4: Stop and disable the WWW Service and confirm an incident is automatically created by Orchestrator**

1. Log on to LON-MS1, click **Start**, and then click **Administrative Tools**.
2. In the **Administrative Tools** window, double-click **Services**.
3. In the **Services** window, right-click **World Wide Web Publishing Service**, and then click **Properties**.
4. In the **World Wide Web Publishing Service Properties** window, click the **Startup type** drop-down menu , and then click **Disabled**.
5. Under **Service status**, click **Stop**.
6. Click **Ok** on the **World Wide Web Publishing Service Properties** window.
7. Open the Operations console, and then click the **Monitoring** pane.
8. Click **Active Alerts**, and then wait for the **IIS 8 Web Site is unavailable** alert to appear.
9. Log on to LON-SM1, and then open the Service Manager Console.
10. Click the **Work Items** pane, and then expand **Incident Management**.
11. Click **All Incidents**, and then from the **Details pane**, confirm that the **Failed to restart Web Site** incident was automatically created by Orchestrator.
12. Log on to LON-MS1, click **Start**, and then click **Administrative Tools**.

13. In the **Administrative Tools** window, double-click **Services**.
14. In the **Services** window, right-click **World Wide Web Publishing Service**, and then click **Properties**.
15. In the **World Wide Web Publishing Service Properties** window, click the **Startup type** drop-down menu, and then click **Automatic**.
16. Click **Apply**.
17. Under **Service status**, click **Start**.
18. Close the **World Wide Web Publishing Service Properties** window.

**Results:** During this exercise, you imported an Orchestrator runbook. The runbook should detect when a default website is unavailable, and then automatically restart it. If the runbook cannot automatically restart the website, the runbook creates an incident in Service Manager. You tested this integration by first stopping the default website on LON-MS1, and then confirming that the website restarted automatically. You then stopped and disabled the WWW service. This made it impossible for the website to be started. Then you confirmed that an incident was automatically created in Service Manager.

# Module 11: Troubleshooting, Tuning, and Disaster Recovery

## Lab: Troubleshooting Operations Manager

### Exercise 1: Troubleshooting an Agent Installation Failure in Operations Manager

#### ► Task 1: Uninstall the Operations Manager agent from LON-DC1

1. On LON-MS1, open the Operations console.
2. Click the **Administration** pane, expand **Device Management**, and then click **Agent Managed**.
3. From the details pane, right-click LON-DC1 and then click **Uninstall**.
4. In the **Uninstall Agents** window that opens, click **Other user account**.
5. In the **User name** box, type **Administrator**; in the **Password** box, type **Pa\$\$w0rd**; and then click **Uninstall**.
6. In the **Agent Management Task Status** window that opens, wait until the **The task completed successfully** message appears, and then click **Close**.

#### ► Task 2: Attempt to install the agent on LON-DC1

1. On LON-MS1 in the Operations console, click the **Administration** pane, and then click **Discovery Wizard**.
2. In the Computer and Device Management Wizard, that opens, on the **Discovery Type** page, click **Next**.
3. On the **Auto or Advanced** page ensure **LON-MS1.CONTOSO.COM** is selected under the **Management Server** section and then click **Next**.
4. On the **Discovery Method** page, in the **Browse for, or type-in computer names** box, type **LON-DC1**; and then click **Next**.
5. On the **Administrator Account** page, click **Discover**.
6. On the **Select Objects to Manage** page, select the **LON-DC1.CONTOSO.COM** check box, and then click **Next**.
7. On the **Summary** page, click **Finish**.
8. In the **Agent Management Task Status** window that opens, review the **Task Output** information, and note the **Access is denied** message.
9. Click **Close**.

#### ► Task 3: Fix the problem on LON-DC1

1. Log on to LON-DC1, click **Start**, click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In **Active Directory Users and Computers**, expand **CONTOSO.COM** and then click **Builtin**.
3. From the details pane, right-click **Administrators**, and then click **Properties**.
4. In the **Administrators Properties** window that opens, click the **Members** tab and then click **Add**.
5. In the **Select Users, Contacts, Computers, Service Accounts or Groups** window that opens, in the **Enter the object names to select** box, type **svc\_SCOM2012\_MSAA**, and then click **Check Names**.

6. In the **Select Users, Contacts, Computers, Service Accounts or Groups** window, click **OK**, and then in the **Administrators Properties** window, click **OK**.
7. Close **Active Directory Users and Computers**, and then log off LON-DC1.

► **Task 4: Install the Operations Manager agent on LON-DC1**

1. On LON-MS1, in the Operations console, click the **Administration** pane, and then click **Discovery Wizard**.
2. In the **Computer and Device Management Wizard** that opens, on the **Discovery Type** page, click **Next**.
3. On the **Auto or Advanced** page, ensure **LON-MS1.CONTOSO.COM** is selected under the **Management Server** section and then click **Next**.
4. On the **Discovery Method** page, click the **Browse for, or type-in computer names** box, type **LON-DC1**, and then click **Next**.
5. On the **Administrator Account** page, click **Discover**.
6. On the **Select Objects to Manage** page, select the **LON-DC1.CONTOSO.COM** check box, and then click **Next**.
7. On the **Summary** page, click **Finish**.
8. In the **Agent Management Task Status** window that opens, review the **Task Output** information, and note the **The task completed successfully** message.

**Results:** After this exercise, you should have reviewed the task output log in the Operations console to determine the cause of the agent installation failure. You should have then resolved the problem that caused the installation failure and successfully installed the Operations Manager agent.

## Exercise 2: Recovering from a Management Server Failure

### ► Task 1: Build a new Management Server

1. Shut down **LON-MS2** to simulate a **Management Server** failure.
2. On **LON-HOST1** open the **Hyper-V Manager Console** and then right-click **LON-HOST1**, then click **New**, then click **Virtual Machine**.
3. In the **New Virtual Machine Wizard** that opens, on the **Before You Begin** page click **Next**.
4. On the **Specify Name and Location** page type **LON-MS2\_New** in the **Name** box and then click **Next**.
5. On the **Assign Memory** page type **1024** in the **Startup memory** box replacing **512** and then click **Next**.
6. On the **Configure Networking** page click the drop-down list next to **Connection** and then click **External Network** and then click **Next**.
7. On the **Connect Virtual Hard Disk** page click **Attach a virtual hard disk later** and then click **Next**.
8. On the **Summary** page click **Finish**.
9. In **Hyper-V Manager** right-click **LON-MS2\_New** and then click **Settings**.
10. In the **Settings for LON-MS2\_New on LON-HOST1** window that opens click **IDE Controller 0** and then click **Add**.
11. Click **New** and in the **New Virtual Hard Disk Wizard** that opens click **Next**.
12. On the **Choose Disk Format** page click **VHD** and then click **Next**.
13. On the **Choose Disk Type** page click **Differencing** and then click **Next**.
14. On the **Specify Name and Location** page type **LON-MS2\_new.vhd** in the **Name** box and then click **Next**.
15. On the **Configure Disk** page click **Browse** and then browse to **<DriveLetter>:\Program Files\Microsoft Learning\Base** and then click **Base14A-WS12R2.vhd** and then click **Open**.



**Note:** Replace <DriveLetter> with the drive letter of where the extracted base VHD's are located.

16. On the **Configure Disk** page click **Next**.
17. On the **Summary** page click **Finish**.
18. On the **Settings for LON-MS2\_New on LON-HOST1** window click **OK**.
19. On **LON-HOST1**, right-click **LON-MS2\_New**, and then click **Start**.
20. Right-click **LON-MS2\_New**, and then click **Connect**.
21. Wait for the **Settings** window to appear, and then click **Next**.
22. On the **Please read the license terms** page, click **I Accept**.
23. On the **Settings** page, in the **Password** and **Reenter password** boxes, type **Pa\$\$w0rd**, and then click **Finish**.
24. Log on to **LON-MS2\_New** by using the **Administrator** account and the **Pa\$\$w0rd** password.
25. In **Server Manager** window that opens, click **Local Server**.

26. Next to **Computer name**, click the hyperlink.
27. In the **System Properties** window that opens, click **Change**.
28. In the **Computer name** box, remove the existing text, type **LON-MS2**, and then click **OK**.
29. In the **Computer Name/Domain Changes** window that opens, click **OK**.
30. In the **System Properties** window, click **Close**.
31. In the **Microsoft Windows** window that opens, click **Restart Now**.
32. Wait for the computer to restart, and then log on as **Administrator**.
33. In the **Server Manager** window that opens, click **Local Server**.
34. Click the hyperlink next to **Ethernet**.
35. In the **Network Connections** window that opens, right-click **Ethernet**, and then click **Properties**.
36. In the **Ethernet Properties** window that opens, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
37. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window that opens, click **Use the following IP address**.
38. In the **IP address** box, type **10.10.0.65**.
39. In the **Subnet mask** box, type **255.0.0.0**.
40. In the **Default Gateway** box, type **10.10.0.1**.
41. In the **Preferred DNS Server** box, type **10.10.0.10**, and then click **OK**.
42. In the **Ethernet Properties** window, click **Close**.
43. Close the **Network Connections** window.
44. In Server Manager, next to **Workgroup**, click the hyperlink.
45. In the **System Properties** window that opens, click **Change**.
46. In the **Computer Name/Domain Changes** window that opens, click **Domain**.
47. In the **Domain** box, type **Contoso.com**, and then click **OK**.
48. In the **Windows Security** window that opens, in the **User name** box, type **Contoso\Administrator**; in the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
49. In the **Computer Name/Domain Changes** window that opens, click **OK**.
50. In the **Computer Name/Domain Changes** window that opens, click **OK**.
51. In the **System Properties** window, click **Close**.
52. In the **Microsoft Windows** window that opens, click **Restart Now**.
53. Wait for the computer to restart, and then log on as **Contoso\Administrator**.
54. In Server Manager, click the **Tools** menu, and then click **Computer Management**.
55. In the **Computer Management** window that opens, expand **Local Users and Groups**, and then click **Groups**.
56. From the details pane right-click **Administrators** and then click **Properties**.
57. In the **Administrators Properties** window that opens, click **Add**.

58. In the **Select Users, Computers, Service Accounts or Groups** window, in the **Enter the object names to select** box, type **SCOM2012\_Admins**, click **Check Names**, and then click **OK**.

59. In the **Administrators Properties** window, click **OK**.

60. Close Computer Management.

61. Log off LON-MS2\_New.

#### ► Task 2: Recover the Management Server

1. Logon to **LON-MS2\_New** using the **Contoso\Administrator** account.

2. Right-click **Start** and then click **Run**.

3. In the **Run** window that opens type **\LON-DC1** in the **Open** box and then click **OK**.

4. In the LON-DC1 window that opens, right-click **Media**, and then click **Map network drive**.

5. In the **Map Network Drive** window that opens, ensure the **Drive** value is set to **Z**, and then click **Finish**.

6. Right-click **Start**, and then click **Run**.

7. In the **Run** window that opens, in the **Open** box, type **CMD**, and then click **OK**.

8. In the **Administrator: C:\Windows\system32\cmd.exe** window that opens, go to **Z:\SCOM2012R2**.

9. Type the following, and then press Enter on the keyboard.

```
Setup.exe /silent /AcceptEndUserLicenseAgreement /recover /EnableErrorReporting:Never
/SendCEIPReports:0 /UseMicrosoftUpdate:0 /DatabaseName:OperationsManager
/SqlServerInstance:LON-SQ1 /DWDatabaseName:OperationsManagerDW
/DWSqlServerInstance:LON-SQ1 /DASAccountUser:Contoso\svc_SCOM2012_das
/DASAccountPassword: Pa$$w0rd /DatareaderUser:Contoso\svc_SCOM2012_dwread
/DatareaderPassword:Pa$$w0rd /DataWriterUser:Contoso\svc_SCOM2012_dwwrite
/DataWriterPassword:Pa$$w0rd
/ActionAccountUser:Contoso\svc_SCOM2012_msaa
/ActionAccountPassword:Pa$$w0rd
```

10. Open Task Manager, click **More Details** and then click the **Details** tab.

11. Monitor the **Setup.exe** process, and wait for it to disappear.

#### ► Task 3: Confirm the new Management Server is operating

1. On LON-MS1, open the Operations console.

2. Click the **Administration** pane, expand **Device Management**, and then click **Management Servers**.

3. From the details pane, confirm **LON-MS2** is displayed and the **Health State** column displays **Healthy**.

**Results:** After this exercise, you should have built a new virtual machine running Windows Server 2012 and joined it to the Contoso network. You then install the Operations Manager Management Server feature by using the Recover switch. Finally, you confirm the Management Group is operational by using the Operations console.

## Exercise 3: Recovering from an operational database failure

### ► Task 1: Back up the OperationsManager database

1. Log on to LON-MS1, and close the Operations console if it is already open.
2. Log on to **LON-SC1**, click **Start**, and then click **SQL Server Management Studio**.
3. In the **Connect to Server** window that opens, type **LON-SQ1** in the **Server name** box, replacing the exiting text and then click **Connect**.
4. In the **Object Explorer** pane, expand **Databases**, right-click **OperationsManager**, click **Tasks**, and then click **Back Up**.
5. In the **Backup Up Database – Operations Manager** window that opens, click **OK**.
6. In the **Microsoft SQL Server Management Studio** window that opens, click **OK**.
7. Close SQL Server Management Studio.

### ► Task 2: Delete the OperationsManager database

1. Logon to **LON-SC1** and then click **Start** then click **SQL Server Management Studio**.
2. In the **Connect to Server** window that opens, type **LON-SQ1** in the **Server name** box, replacing the exiting text and then click **Connect**.
3. In the **Object Explorer** pane expand **Databases** and then right-click **OperationsManager** and then click **Delete**.
4. In the **Delete Object** window that opens clear the **Delete backup and restore history information** for databases check box.
5. Select the **Close existing connections** check box, and then click **OK**.
6. Confirm the **OperationsManager** database has been removed from the **Object Explorer**.
7. Close **SQL Server Management Studio**.
8. Log on to **LON-MS1**, and then open the **Operations console**.
9. On the **Connecting to Server** process, notice the **Microsoft System Center 2012 R2 Operations Manager** window freezes.
10. Open **Task Manager**; click **More Details** and then from the **Details** tab, right-click the **Microsoft.EnterpriseManagement.Monitoring.Console.exe** process; and then click **End task**.
11. In the **Task Manager** window that opens, click **End process**.

### ► Task 3: Restore the OperationsManager database

1. Log on to **LON-SC1**, click **Start**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** window that opens, type **LON-SQ1** in the **Server name** box, replacing the exiting text and then click **Connect**.
3. In the **Object Explorer** pane, right-click **Databases**, and then click **Restore Database**.
4. In the **Restore Database** window that opens, click **Device**, and then click (...).
5. In the **Select backup devices** window that opens, click **Add**.
6. In the **Locate Backup File – LON-SQ1** window that opens, go to **C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup**, click **OperationsManager.bak**, and then click **OK**.
7. In the **Select backup devices** window, click **OK**.

8. In the **Restore Database – Operations Manager** window, click **OK**.
9. In the **Microsoft SQL Server Management Studio** window that opens, click **OK**.
10. In the **Object Explorer** pane, expand **databases**, and confirm the **OperationsManager** database is visible.
11. Close **SQL Server Management Studio**.
  - **Task 4: Confirm the Management Group is operating as expected**
  - 1. On LON-MS1, click **Start**, and then click **Administrative Tools**.
  - 2. In the **Administrative Tools** window that opens, double-click **Services**.
  - 3. In the **Services** window that opens, right-click **System Center Data Access Service**, and then click **Restart**.
  - 4. Right-click **System Center Management Configuration**, and then click **Restart**.
  - 5. Close the **Services** window.
  - 6. Open the Operations console.
  - 7. Confirm the Operations console opens as expected.

**Results:** After this exercise, you should have backed up OperationsManager database. You should then have deleted the OperationsManager database, which simulates a database failure. You should then have restored the OperationsManager database. Finally, using the Operations console, you should have confirmed that the Operations Manager Management Group is functional.

