

JP1 Version 12

Infrastructure Management: Getting Started

3021-3-D60-30(E)

Notices

■ Relevant program products

P-2A2C-DCCL JP1/Operations Analytics 12-60 (for Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows Server 2019)

■ Trademarks

HITACHI, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

AIX is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

Hyper-V is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft Edge is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Windows Server is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

JP1/Operations Analytics includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from <ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)
2. This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)
3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)
4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

```
-----  
/* =====  
* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.  
*  
* Redistribution and use in source and binary forms, with or without  
* modification, are permitted provided that the following conditions  
* are met:  
*  
* 1. Redistributions of source code must retain the above copyright  
* notice, this list of conditions and the following disclaimer.  
*  
* 2. Redistributions in binary form must reproduce the above copyright  
* notice, this list of conditions and the following disclaimer in  
* the documentation and/or other materials provided with the  
* distribution.  
*  
* 3. All advertising materials mentioning features or use of this  
* software must display the following acknowledgment:  
* "This product includes software developed by the OpenSSL Project  
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"  
*  
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to  
* endorse or promote products derived from this software without  
* prior written permission. For written permission, please contact  
* openssl-core@openssl.org.  
*  
* 5. Products derived from this software may not be called "OpenSSL"  
* nor may "OpenSSL" appear in their names without prior written  
* permission of the OpenSSL Project.  
*  
* 6. Redistributions of any form whatsoever must retain the following  
* acknowledgment:  
* "This product includes software developed by the OpenSSL Project  
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.

* =====

*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

*

* This package is an SSL implementation written

* by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscapes SSL.

*

* This library is free for commercial and non-commercial use as long as

* the following conditions are adhered to. The following conditions

* apply to all code found in this distribution, be it the RC4, RSA,

* lhash, DES, etc., code; not just the SSL code. The SSL documentation

* included with this distribution is covered by the same copyright terms

* except that the holder is Tim Hudson (tjh@cryptsoft.com).

*

* Copyright remains Eric Young's, and as such any Copyright notices in

* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution

* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or

* in documentation (online or textual) provided with the package.

- *
 - * Redistribution and use in source and binary forms, with or without
 - * modification, are permitted provided that the following conditions
 - * are met:
 - * 1. Redistributions of source code must retain the copyright
 - * notice, this list of conditions and the following disclaimer.
 - * 2. Redistributions in binary form must reproduce the above copyright
 - * notice, this list of conditions and the following disclaimer in the
 - * documentation and/or other materials provided with the distribution.
 - * 3. All advertising materials mentioning features or use of this software
 - * must display the following acknowledgement:
 - * "This product includes cryptographic software written by
 - * Eric Young (eay@cryptsoft.com)"
 - * The word 'cryptographic' can be left out if the routines from the library
 - * being used are not cryptographic related :-).
 - * 4. If you include any Windows specific code (or a derivative thereof) from
 - * the apps directory (application code) you must include an acknowledgement:
 - * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- *
 - * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
 - * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 - * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 - * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 - * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 - * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 - * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 - * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 - * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 - * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 - * SUCH DAMAGE.
- *
 - * The licence and distribution terms for any publically available version or
 - * derivative of this code cannot be changed. i.e. this code cannot simply be
 - * copied and put under another distribution licence
 - * [including the GNU Public Licence.]

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://java.apache.org/>).

This product includes software developed by Andy Clark.
Java is a registered trademark of Oracle and/or its affiliates.

HITACHI
Inspire the Next

© Hitachi, Ltd.



Other company and product names mentioned in this document may be the trademarks of their respective owners.

■ Issued

Jan. 2022: 3021-3-D60-30(E)

■ Copyright

All Rights Reserved. Copyright (C) 2019, 2022, Hitachi, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-D60-30(E)) and product changes related to this manual.

| Changes | Location |
|--|----------|
| Microsoft Edge is now supported. | 2.2 |
| The Show Related Resources button was added, and the E2E View window can now be opened from the list of resources associated with a specific port on a switch. | 3.3 |

In addition to the above changes, minor editorial corrections were made.

Contents

Notices 2

Summary of amendments 7

1 Overview 10

- 1.1 What you can do with JP1/OA 11
- 1.2 What is explained in this manual 13
- 1.3 Reading this manual 15

2 Installation and configuration 17

- 2.1 Workflow for installation and configuration 18
- 2.2 Installation prerequisites 19
- 2.3 Installing JP1/OA 21
- 2.4 Logging in to JP1/OA 22
- 2.5 Configuring JP1/OA 23
 - 2.5.1 Creating a user account 23
 - 2.5.2 Configuring the mail server 24
 - 2.5.3 Registering management targets 26
 - 2.5.4 Associating managed targets with users 32
 - 2.5.5 Configuring device monitoring 35
 - 2.5.6 Configuring email notification 38

3 Analyzing and resolving problems 40

- 3.1 Workflow for recognizing and resolving problems 41
- 3.2 Recognizing the problem and identifying the target of the analysis 42
 - 3.2.1 Recognizing problems by using JP1/OA 42
 - 3.2.2 Recognizing problems from notifications from a customer or operator 43
- 3.3 Analyzing bottlenecks 45
- 3.4 Analyzing the impact and severity of a problem 48
- 3.5 Analyzing cause and identifying corrective actions 49
 - 3.5.1 Analyzing the cause 49
 - 3.5.2 Removing the cause 51
- 3.6 Reporting the solution 53

4 Analyzing problems with an application as the starting point 54

- 4.1 Workflow for recognizing and resolving problems by using applications as a starting point 55
- 4.2 Recognizing a problem from a JP1/IM event notification 56
- 4.3 Analyzing events to identify the configuration element that has a problem 57

5 Analyzing problems by analyzing correlations in performance data 60

5.1 Workflow for analyzing problems by analyzing correlations in performance data 61

5.2 Analyzing problems by analyzing correlations in performance data 62

Appendixes 69

A Using the product more efficiently 70

B Version Changes 71

B.1 Changes in version 12-60 71

B.2 Changes in version 12-50 71

B.3 Changes in version 12-10 71

B.4 Changes in version 12-00 71

B.5 Changes in version 11-50 71

B.6 Changes in version 11-10 72

C Reference material for this manual 73

C.1 Related publications 73

C.2 Microsoft product name abbreviations 73

C.3 Conventions: Fonts and symbols 73

C.4 Conventions: Abbreviations for product names 74

C.5 Conventions: Acronyms 75

C.6 Conventions: KB, MB, GB, and TB 75

Index 76

1

Overview

This chapter describes what you can do with JP1/Operations Analytics and what is explained in this manual.

1.1 What you can do with JP1/OA

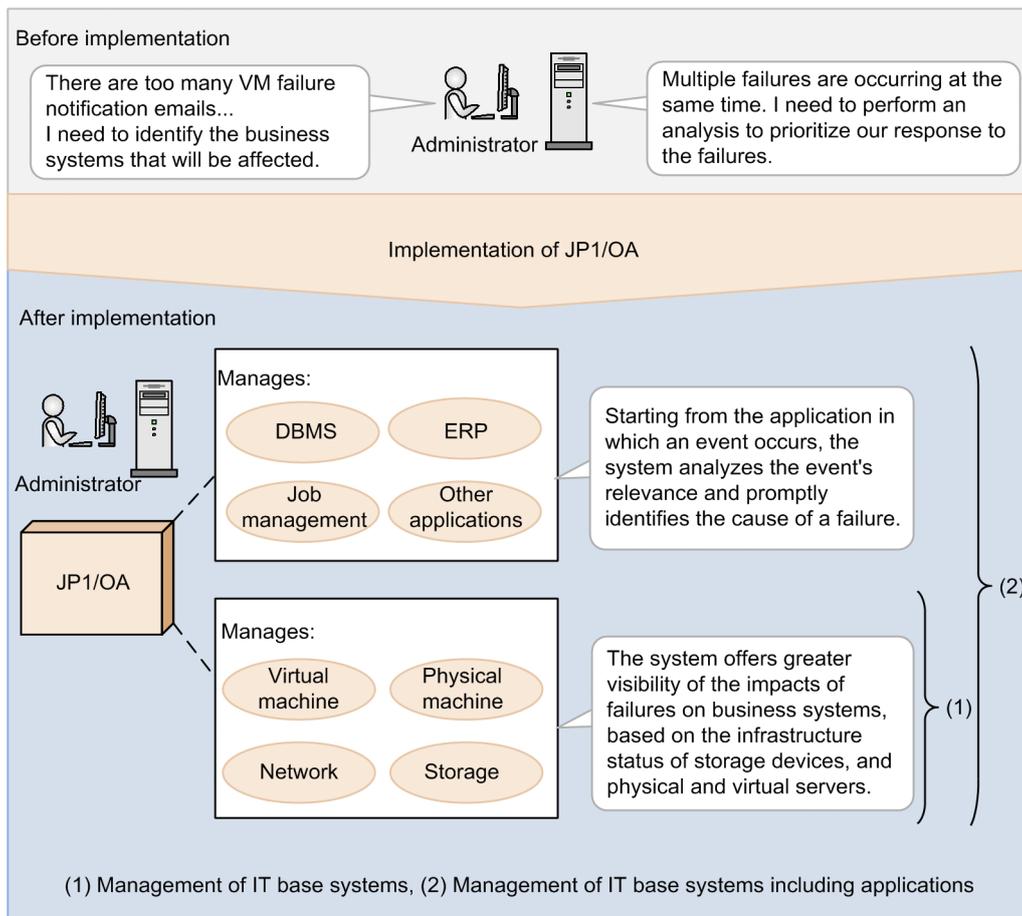
The consolidation and virtualization of IT-base system servers, as well as an increase in the number of applications used to manage business operations, has complicated system configuration work, leading to an increase in what needs to be monitored. After implementing cloud computing to optimize your IT investments, do you have to spend a lot of time trying to understand the entire IT base system?

By introducing JP1/OA, you can get an overview of the operating information of complicated IT base systems. In addition, by simply selecting a device displayed in JP1/OA, you can check the configuration information for the business systems using that device and the configuration information for related devices. Furthermore, monitoring the applications from JP1/OA enables you to get an overview of the status of IT base systems, including applications started from an application in which a JP1 event occurs.

Thus, if a failure occurs in the IT base system, you can isolate the degree of impact and urgency for the failure based on the configuration information for the entire IT base system and take the appropriate action.

In addition, if you receive an inquiry from a customer but no failure has occurred, or if many failures have occurred in the IT base system, do you always know which analysis you should perform first? With JP1/OA, you can identify problematic locations by analyzing the correlation between the performance data of each resource. This allows you to quickly determine the degree of impact and severity of each problem, and to take the appropriate action.

With JP1/OA, you can spend less time managing your entire IT base system and instead spend more time on your business.





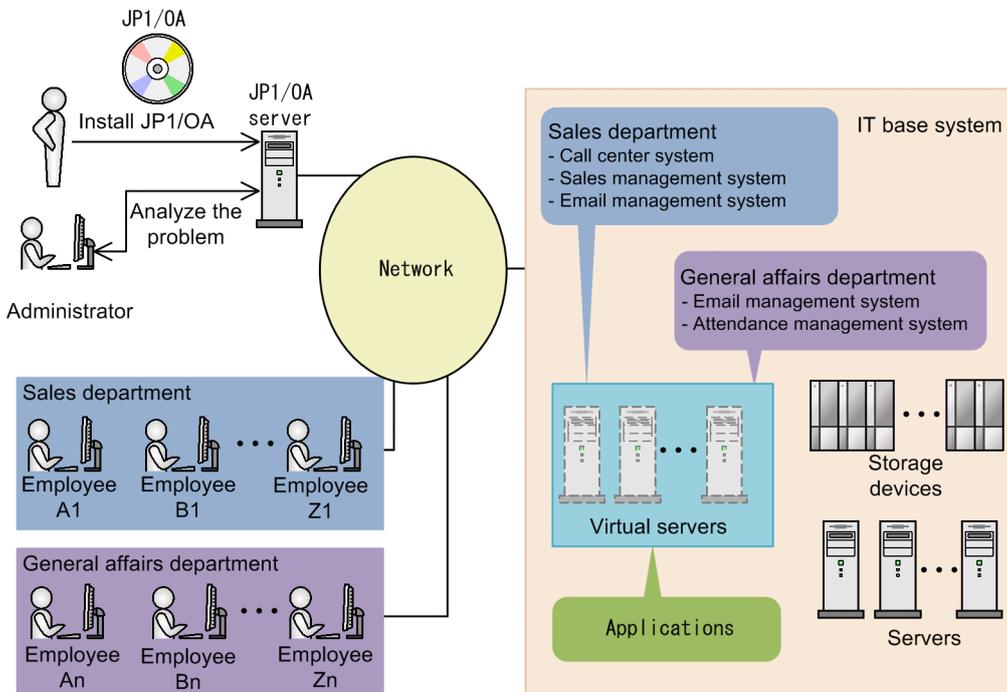
Note

For details about the resources managed by JP1/OA and the performance information to be collected, see the *JP1/Operations Analytics Configuration and Administration Guide*.

1.2 What is explained in this manual

This manual provides an example of how to recognize a problem that has occurred in an IT base system (whose configuration is shown in the figure below) in each of the following cases and how to identify the target of analysis.

- Emails sent by JP1/OA
- Requests from customers or operators to check the operational status or to look into a problem
- Event information from JP1/IM



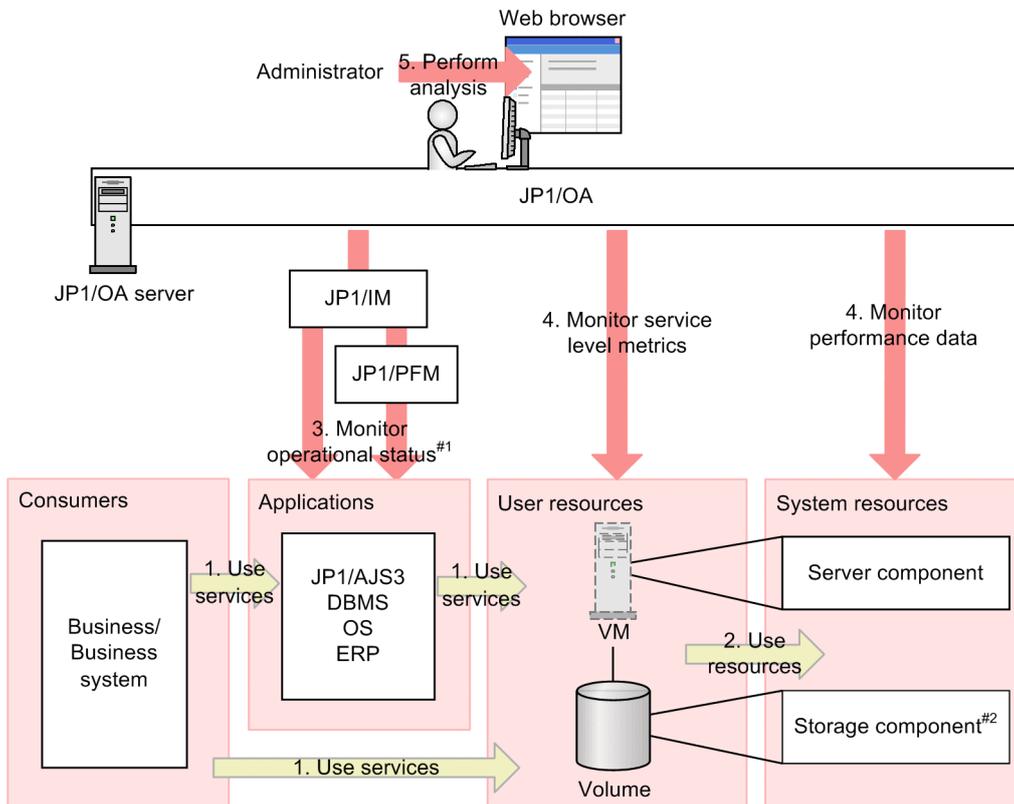
If a problem occurred in the IT base system, use JP1/OA to do the following:

- Analyze the bottleneck
- Analyze the impact and problem severity
- Analyze the cause

If you are monitoring applications, do the following in addition to the above analyses:

- Analyze the relevance of events that occurred in an application, and identify the event that causes a problem.
- Analyze the relevance between the identified event and user resource performance information.

The resources to be used in the analyses and the workflow for the analyses using those resources are as follows:



#1: The operational status of applications is monitored through JP1/IM and JP1/PFM.
 #2: Storage components are not monitored by JP1/OA.

1. Consumers use user resources directly or through applications.
2. User resources use system resources.
3. JP1/OA monitors, through JP1/IM and JP1/PFM, the operational status of applications to check whether they operate normally.
4. JP1/OA monitors user resources and system resources. JP1/OA monitors user resources by using service level metrics and monitors system resources based on performance data.
5. JP1/OA uses this monitoring information to analyze problems.

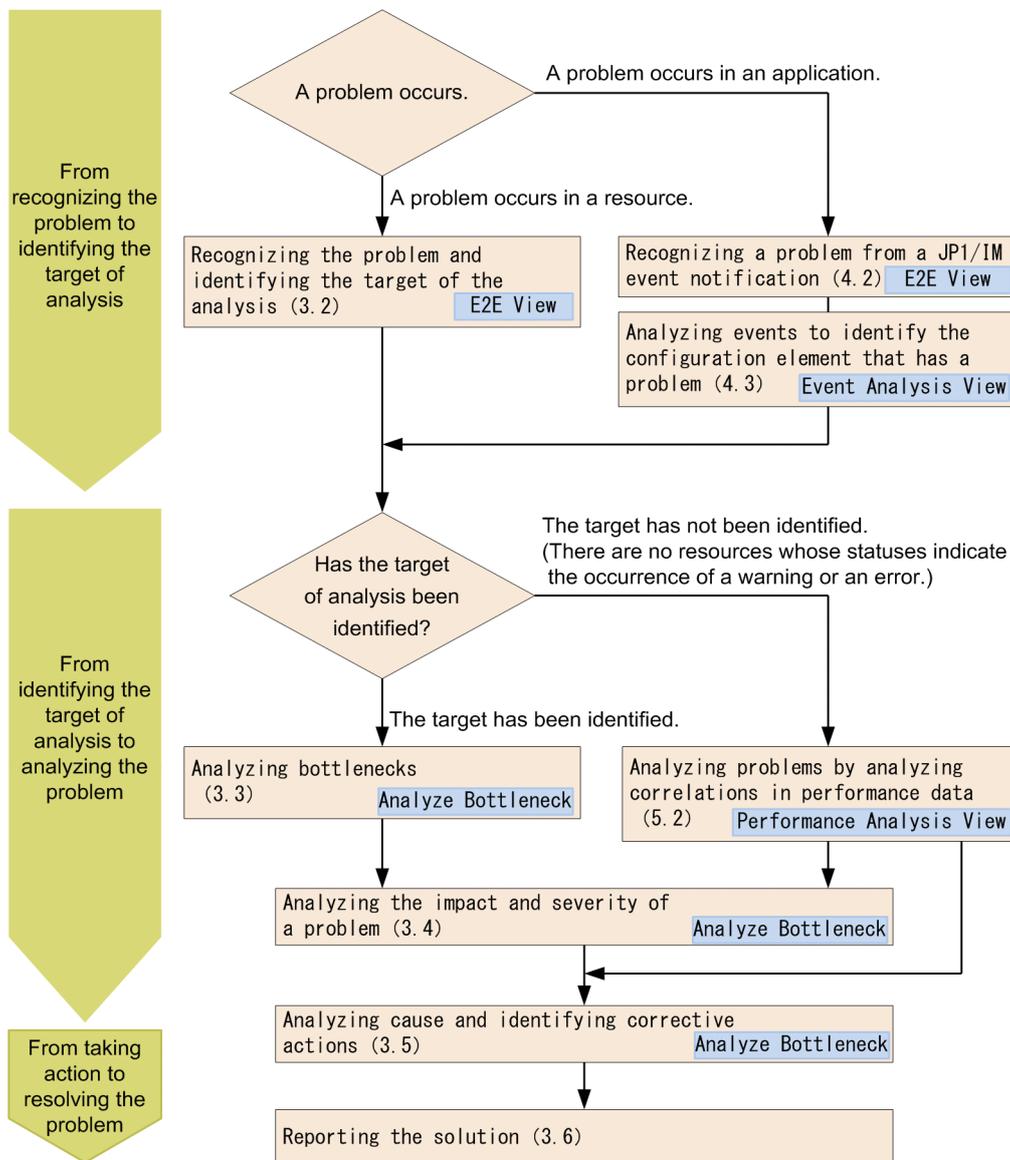
The following table explains the meanings of the terms "consumer", "application", "user resource", and "system resource".

| Term | Meaning |
|-----------------|--|
| Consumer | A customer of a company, department, or business system that uses the application or IT resources. |
| Application | Software that operates on IT resources (such as JP1/AJS3 or DBMS that consumers use) |
| User resource | An IT resource (a logical resource such as a VM or volume) that is used by consumers |
| System resource | An IT resource (a physical resource such as a server or storage device) that is used by user resources |

1.3 Reading this manual

This manual gives an overview of JP1/OA and a basic use of the product.

The following figure shows the main workflow from analyzing problems to resolving problems by using JP1/OA.



Note

Each view window displays the guidance menu on the left side of the window. If you align the cursor with the menu item, guidance on the analysis procedure is displayed.

The following environments are required for operations in each window:

Server on which JP1/OA is installed

Environment that uses Windows Server 2012 R2

Operations performed on the computer of the administrator

Environment that uses Windows 10 and Firefox ESR 91

Due to improvements of the product, note that some of the windows used in this manual might differ from the windows of your product.

2

Installation and configuration

This chapter describes how to install JP1/OA and set up the operating environment in preparation for monitoring an IT base system.

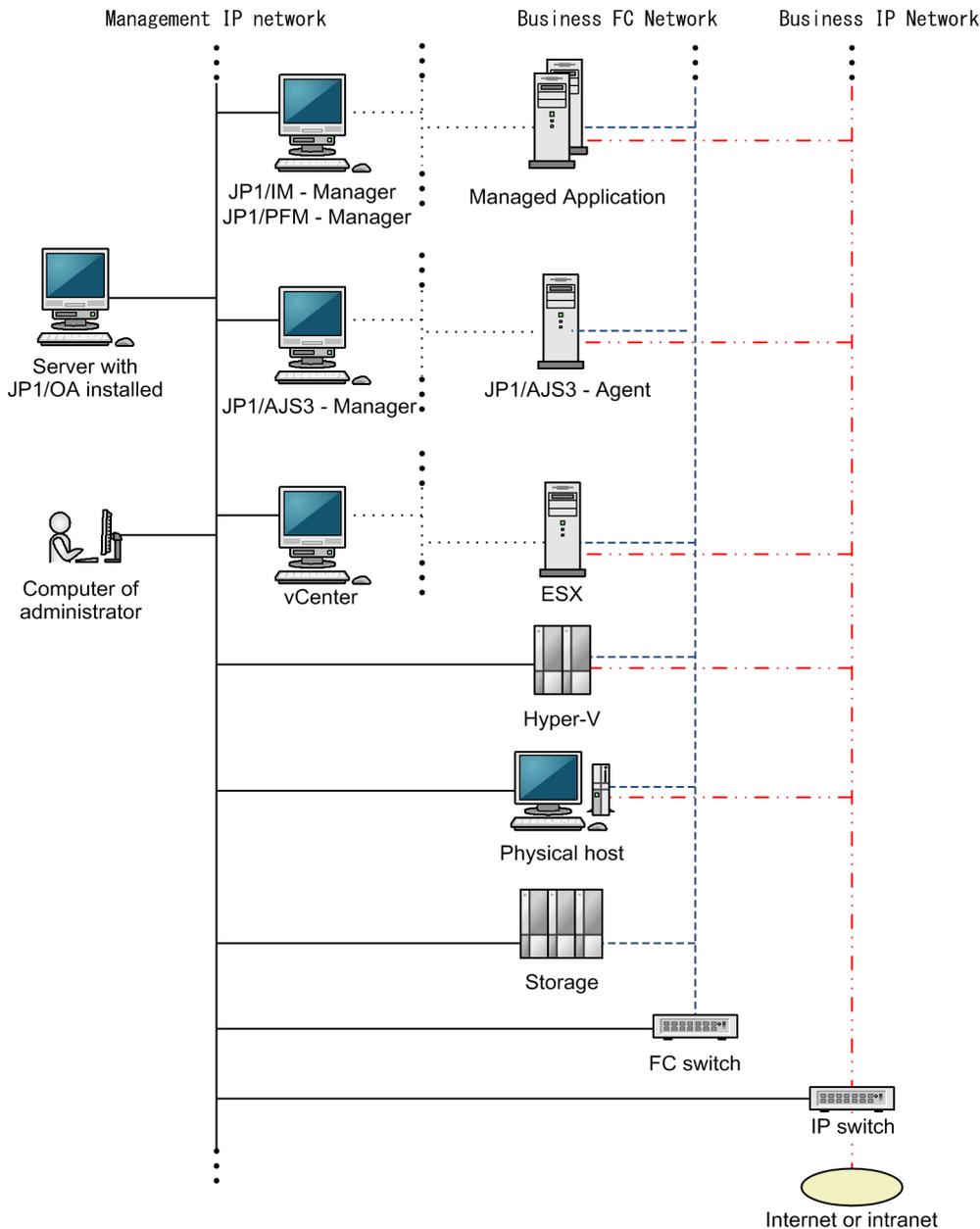
2.1 Workflow for installation and configuration

The workflow for installing and configuring JP1/OA is as follows:

| No. | Procedure |
|-----|--------------------------------|
| 1 | 2.2 Installation prerequisites |
| 2 | 2.3 Installing JP1/OA |
| 3 | 2.4 Logging in to JP1/OA |
| 4 | 2.5 Configuring JP1/OA |

2.2 Installation prerequisites

This section describes the checks you need to perform before installing JP1/OA. The following figure shows the specific elements of the system that need to be checked before installation:



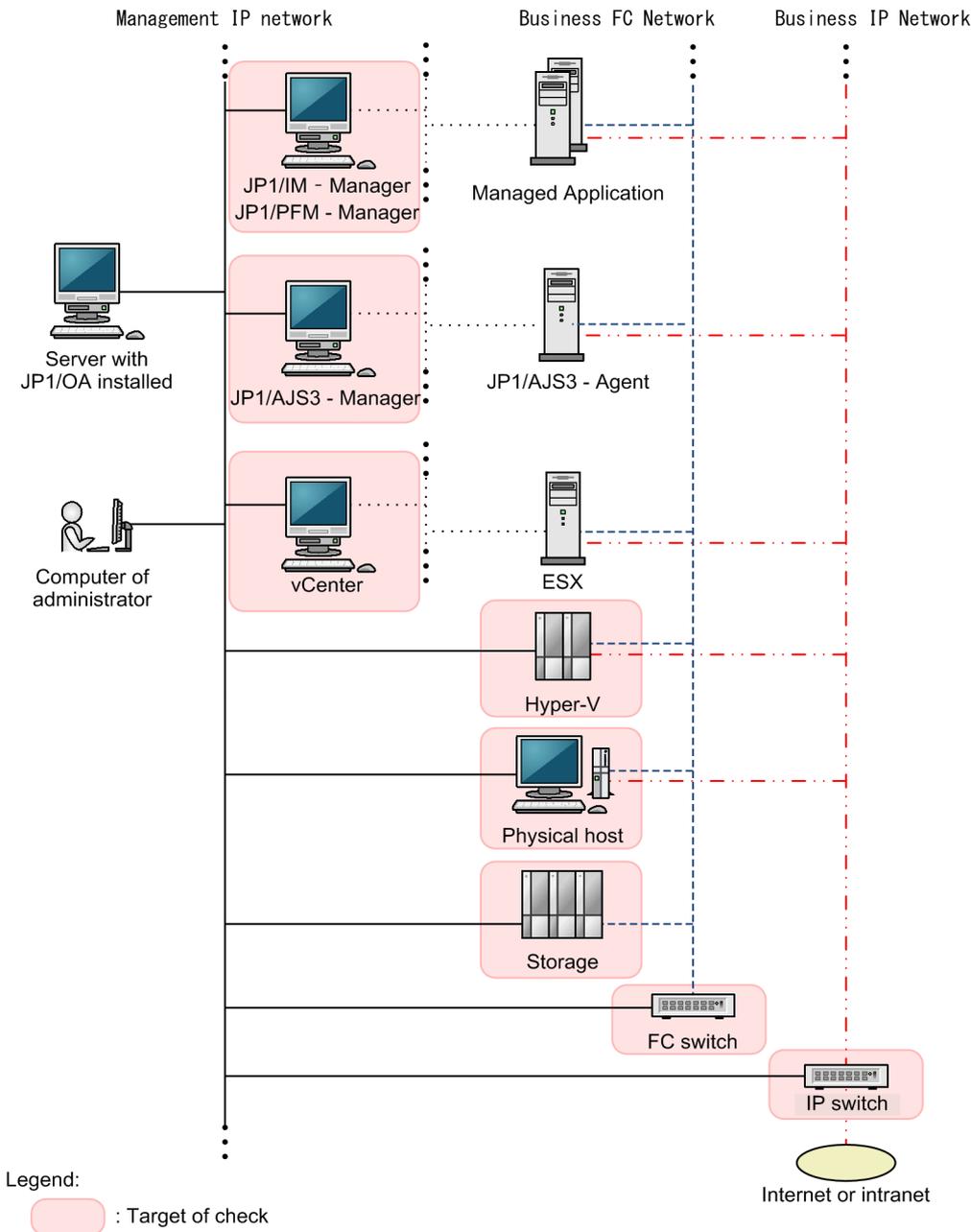
Procedure

1. Reference the sizing information published on the JP1 support page, and select an appropriate configuration according to the scale of the monitoring target. This manual assumes a medium-scale environment to be monitored. Make sure that the server on which JP1/OA will be installed satisfies the following conditions:

- Physical memory: 16.0 GB or more
- Free disk space: 180 GB or more

- CPU: 4 or more cores
- OS: Windows Server 2012 or later

2. Make sure that the server on which JP1/OA will be installed has network access to targets of check which have direct connection to JP1/OA.



3. Check the following aspects of the computer of the server administrator:

- Web browser: Google Chrome 78 or later, Firefox ESR 91, Internet Explorer 11, or Microsoft Edge (Chromium version)
- Web browser language settings: Make sure that the language with the highest priority in the Web browser (English (en) or Japanese (ja)) is the language of the operating system.

2.3 Installing JP1/OA

This section describes how to install JP1/OA on the computer where you want JP1/OA to operate.

Procedure

1. Log on to the machine where JP1/OA is to be installed as a member of the Administrators group, and close all programs.

All programs must be closed when you install JP1/OA.

2. Place the installation media in the drive, and install the product by following the prompts in the installer.

When you install JP1/OA, the following installation folder is created by default:

Installation folder: C:\Program Files\HITACHI\JP1OA

Note that the folder you specify as the installation folder for JP1/OA must be on a fixed disk. You cannot install the product to a removable disk, network drive, or UNC path.

2.4 Logging in to JP1/OA

This section describes how to log in to JP1/OA from the Web browser of the administrator, and then change the password.

Procedure

1. From the Web browser of the administrator, connect to the JP1/OA server.

Enter the following URL in the address bar:

`http://IP-address-of-server-with-JP1/OA-installed:22015/Analytics/login.htm`



Note

You can make the login process easier in the future by bookmarking this URL.

2. Enter the following information in the Login window:

- **User ID:** system
- **Password:** manager

3. Click **Log In**.

You are logged in, and the **Dashboard** window appears.

4. Prepare to change the password of the administrator by selecting the **Administration** tab, and then selecting **User Management** and then **Users and Permissions** in the left pane.

5. In the **Users and Permissions** dialog box, click **Users** to display the user list, and then select **System**.

6. Click **Change Password** and change the password.

2.5 Configuring JP1/OA

Follow the workflow steps in the order specified below to configure the JP1/OA environment successfully.

| No. | Procedure |
|-----|--|
| 1 | 2.5.1 Creating a user account |
| 2 | 2.5.2 Configuring the mail server |
| 3 | 2.5.3 Registering management targets |
| 4 | 2.5.4 Associating managed targets with users |
| 5 | 2.5.5 Configuring device monitoring |
| 6 | 2.5.6 Configuring email notification |

2.5.1 Creating a user account

This section describes how to register users of JP1/OA and assign permissions that govern the range of operations each user can perform. The permissions you can assign are the Admin and Modify permissions for JP1/OA, and the User Management permission. A user with the Admin permission in JP1/OA can perform any operation in JP1/OA. A user with the Modify permission in JP1/OA cannot perform any operation that requires a connection to an external system, such as registering or deleting a management target. A user with the User Management permission can perform operations related to user management, such as registering users and assigning permissions.

Procedure

1. In the **Administration** tab, select **User Management** and then **Users and Permissions**.

- In the **Users and Permissions** dialog box, click **Users** to display a list of users. Then, click **Add User** and enter the required information in the **Add User** window.

Operations Analytics

Add User Help

User Profile

Please enter a value into each field.

2. *User ID: user01

*Password: *****

*Verify Password:

Full Name:

E-mail:

Description:

*Required field

3. OK Cancel

- Click **OK**.

The account is added.



Tip

We recommend that you create a separate account for each user. Preventing the sharing of user accounts results in a more secure system.

- Select the account you added in the left pane of the **User and Permissions** window, and then click **Change Permission**.
- Edit the permission and then click **OK**.
- Log in to JP1/OA using the account you created.
The user whose permission you changed can now perform operations within the scope of the assigned permission.

Next steps

Configure the mail server.

2.5.2 Configuring the mail server

Set up a mail server to notify the administrator by email when a problem occurs in the IT base system or when there is important information that requires their attention.

Before you begin

You must have the Admin permission of JP1/OA to perform this procedure.

Procedure

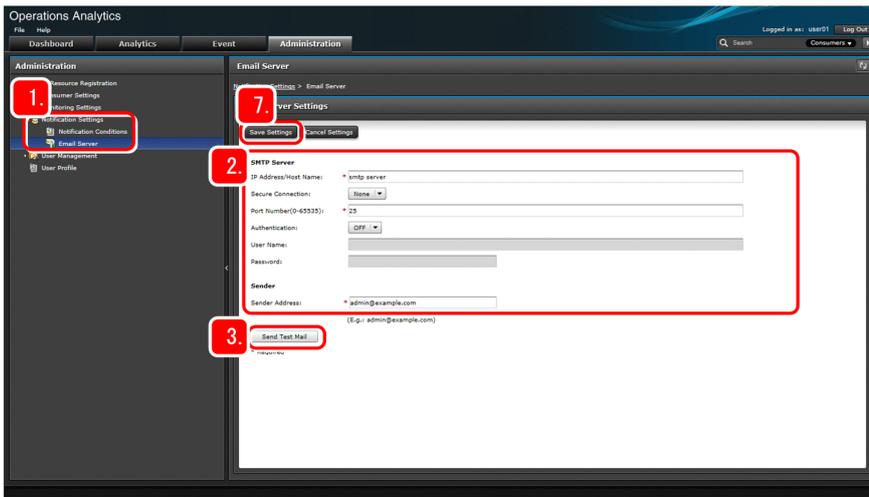
1. In the **Administration** tab, select **Notification Settings** and then **E-mail Server**.
2. Click **Edit Settings** and enter the following information:

SMTP Server

- **IP Address/Host Name:** Name of the host using the email server
- **Secure Connection:** **TLS** (when using secure communication) or **None** (when not using secure communication)
- **Port number (0-65535):** Port number used for communicating with the email server
- **Authentication:** **ON** (when using user authentication) or **OFF** (when not using user authentication)
- **User Name:** User ID associated with the mail server
- **Password:** Password associated with the mail server

Sender

- **Sender Address:** The email address to display in the sender field.
Specify the email address of the administrator in email address format. The address `admin@example.com` will be used as an example in this manual.



3. To confirm that the mail server is set up correctly, click **Send Test Mail**.
4. In the **Send Test Mail** window, specify the email address of the recipient and then click **OK**.
In this case, specify the email address of the administrator.
This email address is not used for any purpose other than sending a test email.
5. Click **Close**.
6. Check whether the test email has arrived in the mailbox of the administrator.
The test email will have the subject line `[Test][JP1/OA-host-name] Analytics test email`.
7. If the test email was received successfully, in the **E-mail Server Settings** window, click **Save Settings**.

Next steps

In JP1/OA, register the devices (management targets) that you want JP1/OA to manage.

2.5.3 Registering management targets

In JP1/OA, devices such as storage systems, servers, and switches are referred to as management targets. By registering these devices and applications, you enable monitoring of these devices and applications.

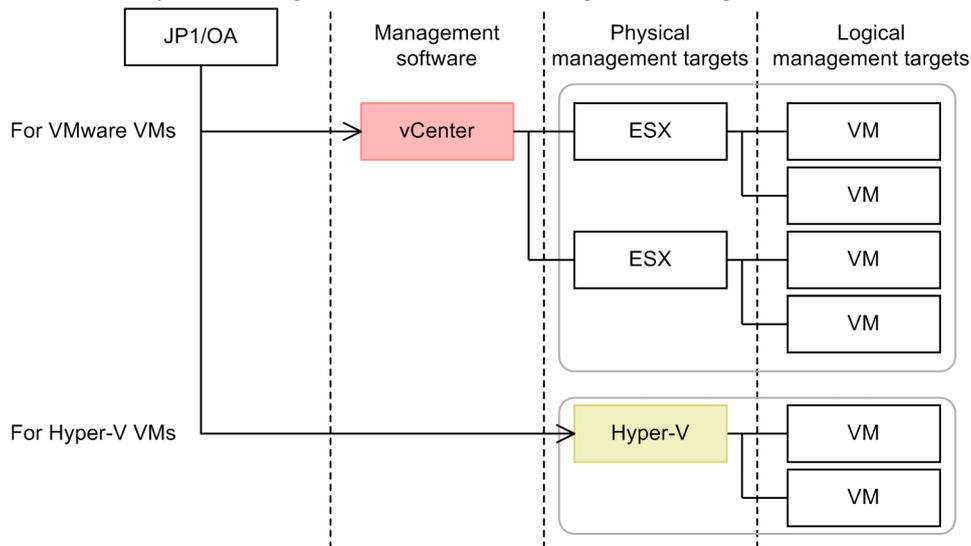
(1) Device configuration

There are two methods you can use to register managed devices: management tool registration and discovery. The management tool registration method allows you to register the management software that you are currently using to manage the devices or applications. The discovery method allows you to register the devices directly. When you use the management tool registration method to register management software, every device or application that is managed by the registered software is registered as a management target in JP1/OA. When you use the discovery method, the administrator can decide whether to register individual devices as management targets on a case-by-case basis.

Selecting a registration method

Whether you use the management tool registration or discovery method depends on the type of device you are registering as a management target.

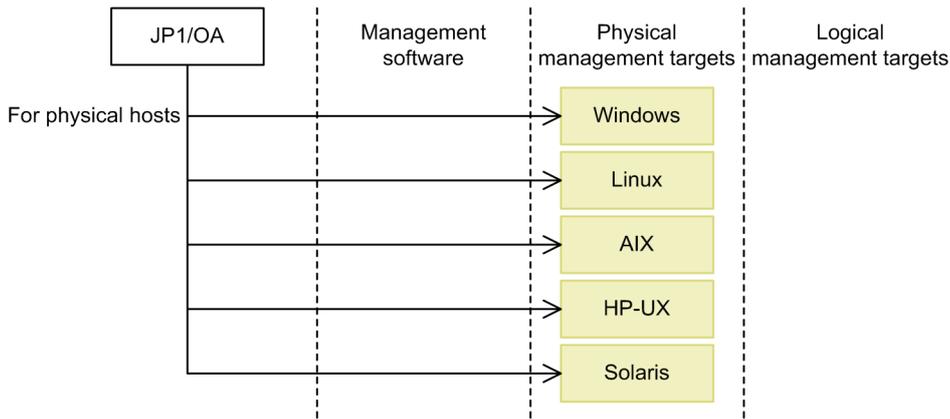
When the device you want to register is a VM, use the following method to register the device:



Legend:

-  : Management software registered by Collector method
-  : Device registered by Discovery method
-  : The range of subordinate devices that automatically become management targets when  or  is registered

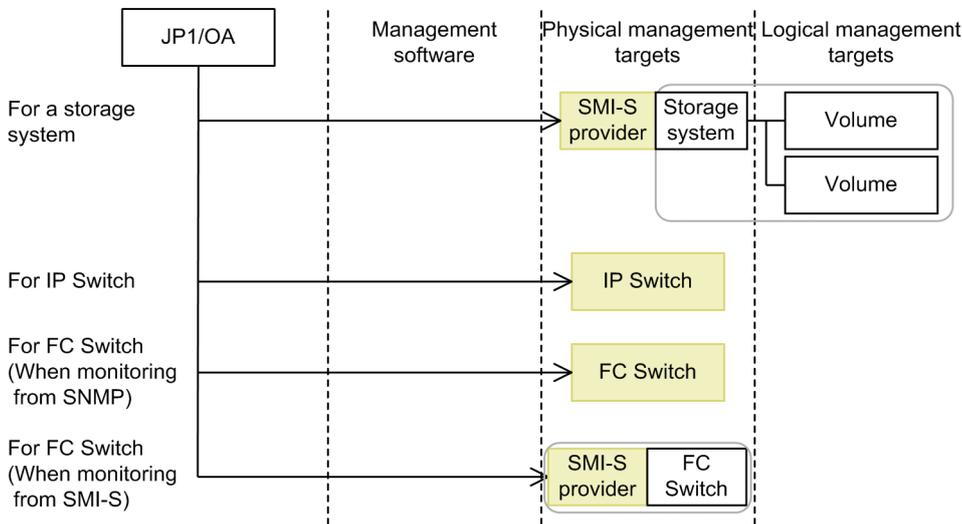
When the device you want to register is a physical host, use the following method to register the device:



Legend:

: Devices registered by Discovery method

- When the device you want to register is a storage system, IP Switch, or FC Switch

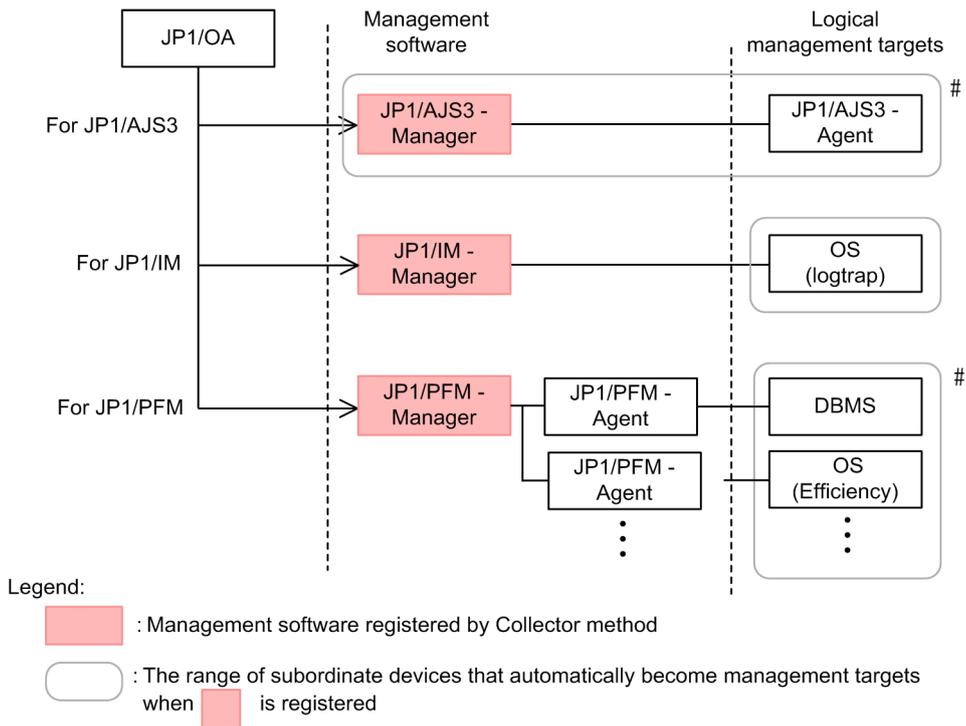


Legend:

: Device to be registered by using the discovery method

: The range of devices automatically registered as management targets when you perform registration

• When you want to register an application, use the following method to register the device:



JP1/IM is required for monitoring JP1 events issued by JP1/AJS3 or JP1/PFM.

Registration method

The table below shows which method you can use to register a device as a management target in JP1/OA.

Locate the type of device (resource) you want to register as a management target in JP1/OA in the table, and identify the appropriate registration method.

| Resources | | Management tool registration | Discovery |
|---------------|---------|------------------------------|-----------|
| VM | VMware | Yes | No |
| | Hyper-V | No | Yes |
| Physical host | | No | Yes |
| Storage | | No | Yes |
| IP switch | | No | Yes |
| FC switch | | No | Yes |
| Application | | Yes | No |

(2) Registering vCenter systems using the management tool registration method

You can register a vCenter system by using the management tool registration method, using the **vCenter** tab. Every device that is managed by the registered vCenter system is to be managed in JP1/OA.

Procedure

1. In the **Administration** tab, select **IT Resource Registration** and then **Management Tool Registration**.
2. Select the **vCenter** tab, and click **Add Collector**.
3. Enter the following information in the **Add Collector** window, and then click **OK**.

Add Collector

To manage all hypervisors and VMs that vCenter manages, enable the collector. To confirm the hypervisors and VMs, go to Managed Resources screen.

3. Collector Name: *

IP Address/Host Name: *

Protocol: https

Port: * 443

User ID: *

Password: *

Enable Scheduling

Refresh Data

* Required

3. OK Cancel

4. Confirm that the connection result for the registered software is **Connection Successful**.
5. Repeat steps 2 through 4 to add another vCenter system.
6. In the left pane, select **IT Resource Registration** and then **Resource Management**.
7. In the **Resource Management** window, click each tab in the **Managed Resources** tab and make sure that the devices you registered are displayed.

(3) Registering devices using the discovery method

Use the discovery method to search for devices using an IP address range and credentials, and register them in JP1/OA.

Procedure

1. In the **Administration** tab, select **IT Resource Registration** and then **Discovery**.
2. In the **Discovery** window, select the **Credentials** tab and then click **Add Credential**.
The credentials for connecting to the devices you want to register as management targets are defined.
3. In the **Name** field, enter a name of your choice for identifying the credentials.
4. In the **Target** field, select the appropriate option for the types of device you want to register as management targets.
 - **WMI**: To register Windows or Hyper-V devices as management targets
 - **SSH**: To register Linux, HP-UX, AIX, or Solaris devices as management targets
 - **SNMP**: To register IP switches or FC switches as management targets

- **SMI-S WBEM:** To register storage or FC switch devices as management targets

5. Enter the device credentials and then click **OK**.

The credentials are registered.

6. Repeat steps 2 through 5 to register credentials for each range of devices you want register as management targets.

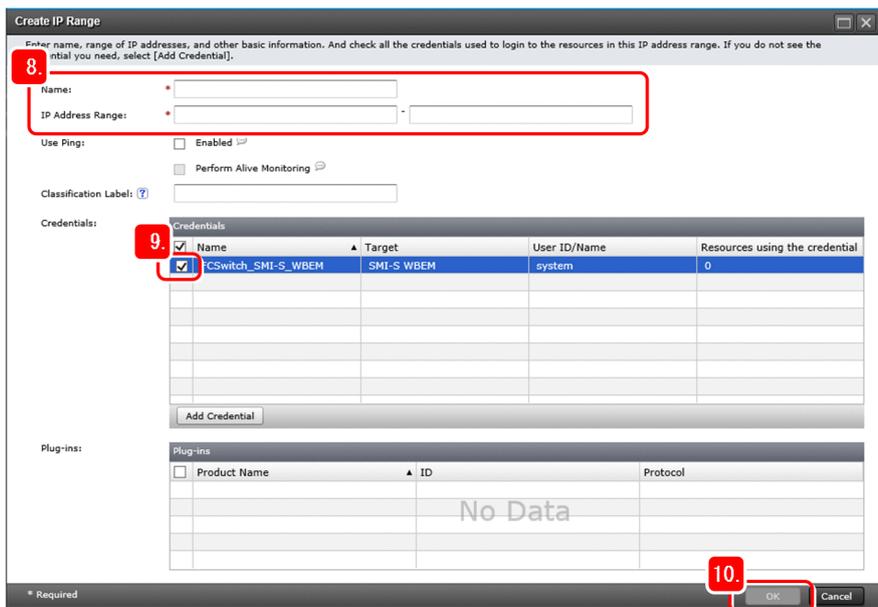
7. In the **Discovery** window, select the **Discovery Settings** tab and then click **Create IP Range**.

8. In the **Create IP Range** dialog box, enter the following items:

- **Name:** A name that represents the IP address range
- **IP Address Range:** The IP address range that contains the devices you want to register as management targets

Note

- If you select **Perform Alive Monitoring**, you can create an IP address range even if you do not specify credentials. However, if you do not specify credentials, you can only monitor whether the connections to the target resources are live. Note that these resources are handled as hosts, and can be associated with consumers and applications.
- If you set a name for **Classification Label**, in the **E2E View** window, you can view hosts grouped by their label name. This is helpful when you want to isolate an environment (for example, to distinguish a cloud environment from an on-premises environment) or perform other tasks.



9. Select the **Credentials** check box for the credentials that apply to the IP address range you registered.

10. Click **OK**.

The specified IP address range and credentials are now linked and registered in the system.

11. Repeat steps 7 through 10 to register more IP address ranges and device credentials.

12. In the **Discovery** window, select the **Discovery Settings** tab and then select the **Name** check boxes for the IP address ranges you registered.

13. Click **Discover Resources**.

To register all devices discovered by the discovery process as management targets (automatic management target registration)

1. Make sure that the **Manage discovered resources automatically** check box is selected.
2. Click **OK**.

To individually select the discovered devices you want to register as management targets (manual management target registration)

1. Clear the **Manage discovered resources automatically** check box.
2. Click **OK**.
3. In the **Resource Management** window, select the **Unconfirmed Resources** tab, select the devices you want to register as management targets, and then click **Manage Resources**.

14. In the **Administration** tab, select **IT Resource Registration** and then **Resource Management**.

15. In the **Resource Management** window, select the **Managed Resources** tab and make sure that the devices you registered as management targets are displayed.

(4) Registering JP1 products to be managed using the management tool registration method

To manage IT base systems including applications, register JP1 products that are linked with the system by executing the management tool registration method from the **Application** tab. All applications managed by the registered JP1 products will be managed in JP1/OA. This manual gives an example of registering JP1 products for Windows.

Before you begin

Either of the following conditions must be satisfied on the Windows server where JP1 products are installed.

- The Windows administrative share is enabled.
- Shared folders are enabled.

Procedure

1. In the **Administration** tab, in the left pane, select **IT Resource Registration** and then **Management Tool Registration**.
2. In the **Application** tab, click the **Add Collector** button.
3. Enter the collector name in the **Add Collector** dialog box, and then select JP1 products to be linked with.
4. Select the type of server on which JP1 products are installed.

5. Enter information and then click **OK**.

* Required



Note

To obtain configuration information about applications from each server, select administrative shares or enter the information about shared folders. For details on how to set Windows administrative shares and how to set shared folders, see *JP1/Operations Analytics Configuration and Administration Guide*.

6. Confirm that the connection result for the registered software is **Connection Successful**.

7. Repeat steps 2 through 6 to register other JP1 products to be linked with.

8. In the left pane, select **IT Resource Registration** and then **Resource Management**.

9. In the **Resource Management** window, click the **Managed Resources** tab and then **application** tab, and make sure that applications to be managed by the JP1 products that you registered using the management tool registration method are displayed.

Next steps

Management-target devices are associated with consumer use of those devices.

2.5.4 Associating managed targets with users

Users of JP1/OA can use a unit called a consumer to group business systems by common attributes, such as the company and department to which they belong or their importance. The concept of a consumer allows an association to be formed between managed targets and consumer use of those targets. This makes it easier to locate a physical or virtual host where a problem has occurred, even when working with multiple consumers each of whom can operate a large-scale business system.

Example of associating devices with users

The following shows an example of business systems of two departments using consumers to associate managed devices (VMs) with consumer use of those devices. This example creates consumers for business systems operated by two departments as shown in the table below.

These consumers group devices by department and by the importance of the business system. Therefore, this example will involve the creation of four consumers.

| Department name | Business system | Importance | VM name | Consumer name |
|----------------------------|------------------------------|------------|---------|--|
| Sales department | Call center system | Critical | VM1 | Sales department (Critical) |
| | | | VM2 | |
| | | | VM3 | |
| Sales department | Sales management system | Important | VM4 | Sales department (Important) |
| Sales department | Email management system | Important | VM5 | |
| General affairs department | Email management system | Important | | General affairs department (Important) |
| General affairs department | Attendance management system | General | VM6 | General affairs department (General) |

In this manual, the importance assigned to a business system has no internal relation to the threshold values you set in [2.5.5 Configuring device monitoring](#).

Procedure

1. In the **Administration** tab, select **Consumer Settings** and then **Consumers**.
2. In the **Consumers** window, click **Create Consumer**, and enter a name for the consumer in the **Consumer Name** field.

For this example, enter Sales department (Critical).

The screenshot shows the 'Create Consumer' dialog box with the following fields and annotations:

- 2.** Consumer Name: Sales department (Critical)
- 3.** Grade: *
- 4.** Description: Company, System, Tel, Address, Contact Person
- 5.** Link: URL
- 6.** Display Name
- 7.** Assign Resources: Applications, VMs, Hypervisors, Hosts, Volumes
- 7.** Add Applications (button)
- 10.** OK (button)

3. Select **Grade**.

The options are Platinum, Gold, Silver, and Bronze, in order from most to least important. The administrator can select the grade most appropriate to the importance of the business system.

For this example, select **Platinum**.

4. In the **Description** text box, enter the company name, business system name, and other information that is helpful to have at hand when communicating with the consumer.

You can specify any other relevant information in the **Description** text box. Adding more details in the **Description** text box might make it easier for administrators to respond to consumer inquiries and resolve issues more quickly.

5. In the **Link** text box, enter the URL of the system where the customer information is managed.

Note that the **Link** text box is useful when the customer information is managed on other Web systems.

6. In the **Display Name** text box, enter the name displayed for the link.

If you did not use the **Display Name** text box, the URL entered in the **Link** text box is displayed without change.

7. Specify **Assign Resources**.

Select the **VMs** tab, and then click the **Add VMs** button.



Note

The following resources are automatically assigned to the consumer. If you want to disable automatic assignment of resources, deselect each option in **Advanced option**.

- Virtual machines that run on a hypervisor that is to be assigned to the consumer
- Applications that run on a virtual machine, or on a host, that is to be assigned to the consumer

8. In the **Available VMs** area of the **Add VMs** window, select check boxes, and then click **Occupy**.

For this example, add the virtual machines you registered in [2.5.3 Registering management targets](#).



Note

In this example, to assign VM5 to Sales department (Important), and then assign it to General affairs department (Important), click **Share**. VM5 is shared between Sales department (Important) and General affairs department (Important).

9. Click **OK**.

10. Make sure that the VMs have been added to the **Manually Selected VMs** list in **Assign Resources**, and then click **OK**.

11. Repeat steps 2 through 10 to register the consumers Sales department (Critical), Sales department (Important), General affairs department (Important) and General affairs department (General).



Note

You can view information about the consumers you registered in the **Consumer Information** dialog box. To display this dialog box, click Consumer in the **Consumers** window.

Next steps

Configure device monitoring.

2.5.5 Configuring device monitoring

You can configure the following device monitoring settings: The conditions you set take effect immediately.

- **Collection intervals**
Sets the monitoring interval for devices. Information will be collected from the registered devices at the set interval.
- **User Resource monitoring conditions**
Sets the conditions to use for detecting deterioration in service performance of monitored VMs and volumes.
- **System Resource monitoring conditions**
Sets the conditions to use for detecting performance bottlenecks in the monitored hardware devices, such as ESX and Hyper-V devices.

(1) Setting the collection intervals

Before you begin

You must have the Admin permission of JP1/OA to perform this procedure.

Procedure

1. In the **Administration** tab, select **Monitoring Settings** and then **Collection Intervals**.
2. In the **Collection Intervals** window, click **Edit Collection Intervals**.

3. Change the conditions in the **Edit Collection Intervals** dialog box.

3.

4.



Note

- After the operation has started, you can check **Last Duration** and **Max Duration** records, and use the records as a reference for adjusting the collection intervals.
- If you have changed the system configuration, click the **Reset Max** button to reset **Max Duration**, and then change **Max Duration** as needed.

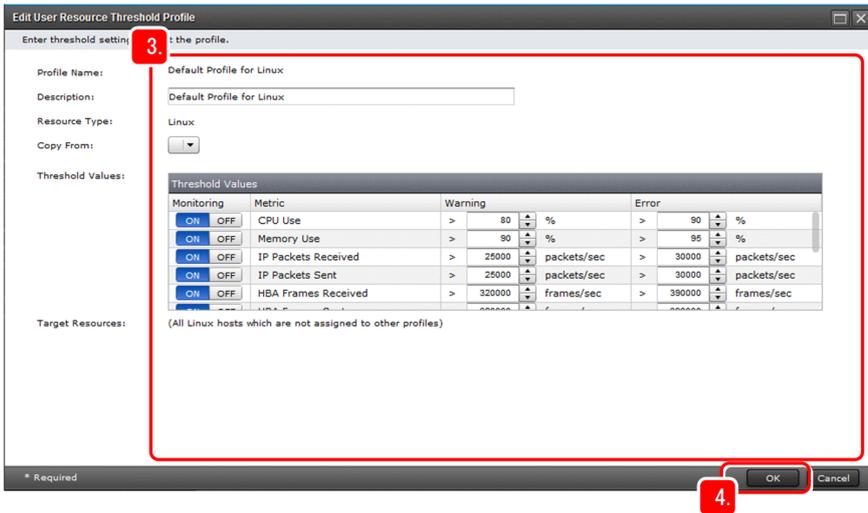
4. Click **OK**.

(2) Setting monitoring conditions for user resources

Procedure

1. In the **Administration** tab, select **Monitoring Settings** and then **User Resource Thresholds**.
2. In the **Profile Name** area of the **User Resource Thresholds** window, select the check box for the profile whose conditions you want to change, and then click **Edit Threshold Profile**.

3. Change the conditions in the **Edit User Resource Threshold Profile** dialog box.

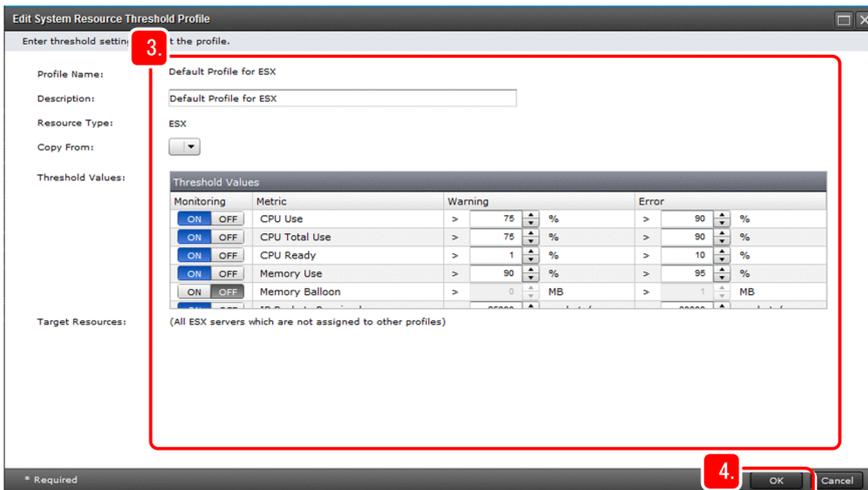


4. Click **OK**.

(3) Setting monitoring conditions for system resources

Procedure

1. In the **Administration** tab, select **Monitoring Settings** and then **System Resource Thresholds**.
2. In the **Profile Name** area of the **System Resource Thresholds** window, select the check box for the profile whose conditions you want to change, and then click **Edit Threshold Profile**.
3. Change the conditions in the **Edit System Resource Threshold Profile** dialog box.



4. Click **OK**.

Next steps

Configure email notification.

2.5.6 Configuring email notification

Configure notification settings for notification events and recipients. By configuring email notification, you can notify the administrator by email of problems in managed business systems and of information that requires their attention.

Before you begin

You must have the Admin permission of JP1/OA to perform this procedure.

Procedure

1. In the **Administration** tab, select **Notification Settings** and then **Notification Conditions**.
2. In the **Notification Conditions** window, select the **Condition Settings** tab and then click **Create Notification Profile**.
3. In the **Create Notification Profile** dialog box, enter a name for the profile in the **Profile Name** field. For this example, specify `Server administration: Manager`.

The screenshot shows the 'Create Notification Profile' dialog box. The 'Profile Name' field is highlighted with a red box and a red '3.' indicating step 3. The 'Add E-mail Address' button is highlighted with a red box and a red '4.' indicating step 4. The dialog box contains the following fields and options:

- Profile Name:** A text input field.
- Description:** A text input field.
- Notification Event Level:** Radio buttons for Error, Error, Warning, and Error, Warning, Information.
- Notification Category:** Radio buttons for All and Specify Categories. Below this is a list of Notification Categories with checkboxes: Category, Performance, Status, Event Action, Setting, and Changes.
- Delivery Address:** A table with columns for E-mail Address, Status, and Description. The table contains two rows: test@example.com (Active) and admin@example.com (Active). Below the table is an 'Add E-mail Address' button.
- E-mail Recipient Type:** A dropdown menu.

At the bottom of the dialog box, there are 'OK' and 'Cancel' buttons, and a '* Required' label.

4. In the **Create Notification Profile** dialog box, click **Add E-mail Address**.
5. In the **E-mail Address** field of the **Add E-mail Address** dialog box, enter the email address of the administrator who will receive notifications, and then click **OK**. For this example, enter the mailing list address `admin@example.com`.

Tip

If you want to change the contents of **Status** or **Description** under **Delivery Address**, you can do so on the **E-mail Addresses** tab of the **Notification Conditions** window.

6. In the **Delivery Address** area of the **Create Notification Profile** dialog box, select the check boxes for the email addresses that you want to enable as recipients of email notifications.
7. Select **E-mail Recipient Type**, and then click **OK**.

8. Make sure that the profile you added appears on the **Condition Settings** tab of the **Notification Conditions** window.



You can create multiple profiles to suit the roles and responsibilities of individual administrators. To add further profiles, repeat steps 2 to 7.

Next steps

Now, we can use JP1/OA to quickly solve a problem that occurred in the system.

3

Analyzing and resolving problems

Use JP1/OA to quickly solve a problem that occurred in the IT base system.

3.1 Workflow for recognizing and resolving problems

The workflow for resolving a problem that occurred in the IT base system is as follows:

| No. | Procedure |
|-----|--|
| 1 | 3.2 Recognizing the problem and identifying the target of the analysis |
| 2 | 3.3 Analyzing bottlenecks |
| 3 | 3.4 Analyzing the impact and severity of a problem |
| 4 | 3.5 Analyzing cause and identifying corrective actions |
| 5 | 3.6 Reporting the solution |

3.2 Recognizing the problem and identifying the target of the analysis

This section describes how to recognize a problem that occurred in the IT base system and how to use JP1/OA to identify which part of the system is affected. This manual describes the procedure for recognizing a problem by using the following, and then identifying the target of analysis:

| No. | In response to | Refer to |
|-----|--|---|
| 1 | Emails sent by JP1/OA | 3.2.1 Recognizing problems by using JP1/OA |
| 2 | Requests from customers or operators to check the operational status or to look into a problem | 3.2.2 Recognizing problems from notifications from a customer or operator |

3.2.1 Recognizing problems by using JP1/OA

This section describes how to recognize a problem and identify the target of analysis in response to an email sent by JP1/OA. Emails are sent to the specified addresses for receiving email notifications from JP1/OA based on the monitoring conditions that were set by using emails from JP1/OA.

Procedure

1. Receive the email from JP1/OA, and then check the information in the email.

The following figure shows an example of an email sent by JP1/OA.

This e-mail notifies you of events detected as of 2015-08-31 10:50:27 +0900.

== Overview ==

| Severity | Number of events |
|----------|------------------|
| Error | 33 |

== Events ==

To see the entire event list, click [here](#).

This information will be analyzed by JP1/OA. This manual provides an example of how to analyze the event where the processing speed of a host has decreased.

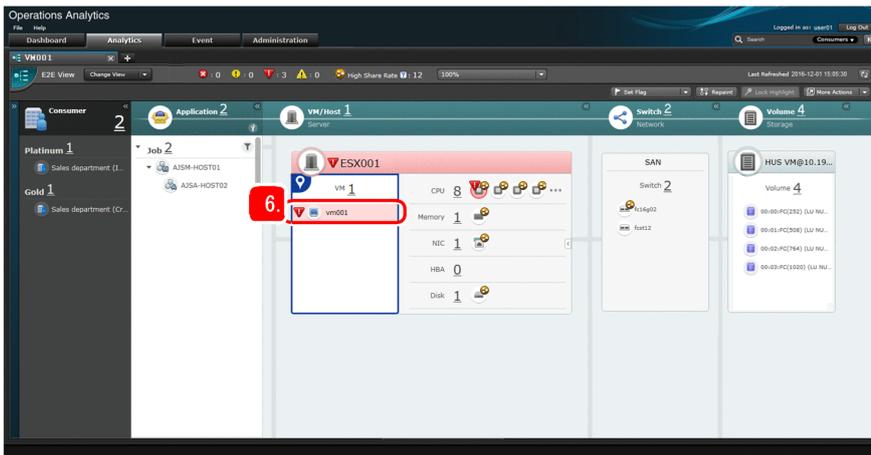
2. Click the link in the email, and then log in to JP1/OA.

The default web browser starts, and the login window appears.

3. Based on the error occurrence date and time in the email, from **Date Time** in the **Event** window, search for the date and time when the problem occurred.
4. Click the **Message** column of the row where "Error" is displayed in **Level**.
5. In the **Event Detail** dialog box, click **Show E2E View**.

In the **E2E View** window, related devices are displayed by using, as the starting point, the problem that occurred. You can use this window to understand the configuration information of the devices related to the problem and to analyze the cause of the problem.

6. In the **E2E View** window, identify the host on which the problem occurred.



Next steps

Analyze the bottleneck by using the information in the email sent by JP1/OA, and from the **E2E View** window. When you receive a notification from a customer or an operator, you can recognize the problem from the information the customer or operator provides.

3.2.2 Recognizing problems from notifications from a customer or operator

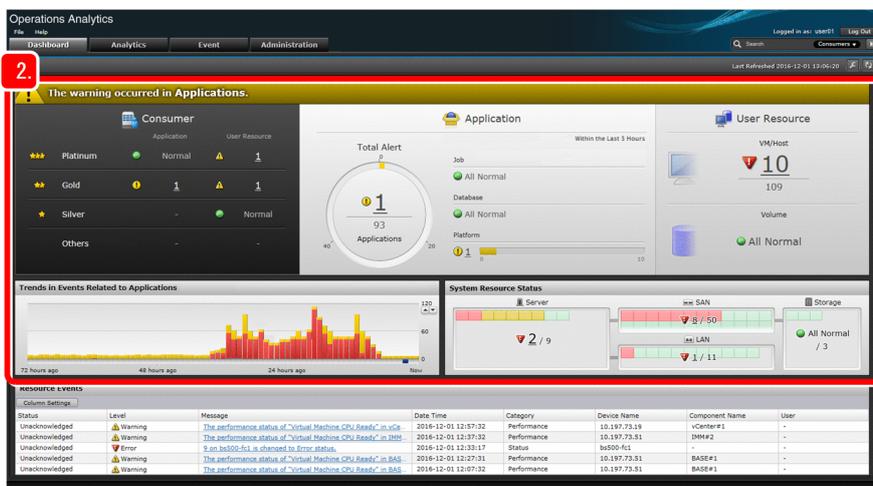
This section describes how to recognize a problem and identify the target of analysis in response to a notification from a customer or from an operator who is monitoring a particular part of the business system. To identify the location of the problem, use the **Dashboard** window. If you cannot identify the location of the problem from the **Dashboard** window, perform a search by using, as keywords, the information provided by the customer or operator.

Procedure

1. Log in to JP1/OA.

The **Dashboard** window appears.

2. Use the **Dashboard** window to check for problems in the part of the business system mentioned in the request from the customer or operator.



3. Analyzing and resolving problems

If a problem has occurred, the number of errors and warnings appears in the **Dashboard** window. For system resources for which the resources to be analyzed need to be identified in advance, the number of errors or warnings is underlined. For user resources for which errors and warnings can be analyzed collectively, >> is displayed on the right side of the number of errors or warnings.

3. Take the following action:

- When there is at least one error or warning

Click the underlined number. In the displayed dialog box, select the resource to be analyzed, and then click **Show E2E View**. In the displayed **E2E View** window, check the problem location. For a number that is not underlined, click >> located to the right of that number and then check the problem location in the **E2E View** window that appears.

If you are able to identify the VM where the problem has occurred, you can skip the subsequent steps. Proceed with the bottleneck analysis.

- When there are no errors or warnings

Perform a keyword search to find the section affected by the problem. Continue with the steps below.

4. In the information acquired from the customer or operator, determine the name of the host where you suspect the problem has occurred.

5. Click the **Analytics** tab.

6. In the text box in the **Analytics** window, enter the name of the host on which the problem is suspected to have occurred.

7. From the drop-down list box for types, select **Servers**, and then click **Search**.

The search results are displayed.

8. In the search results, select the VM affected by the problem.

You can identify whether a VM is affected by the problem based on the information displayed in **Status**.

If you cannot identify a VM affected by the problem from the entered host name, enter a consumer name in **Consumer name** in step 6, select Consumers from the drop-down list box for types in step 7, and then search for a VM to check the problem location.

9. Click **Show E2E View**.

The resource of the business system related to the selected VM appears in the **E2E View** window.

10. Confirm the problem location in the **E2E View** window.

Next steps

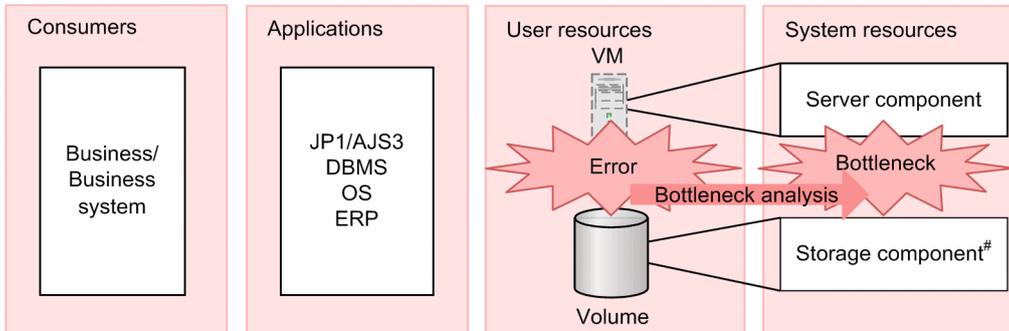
In the **E2E View** window, analyze the bottleneck.

3.3 Analyzing bottlenecks

This section describes how to analyze a bottleneck for a problem that has been identified as an analysis target.

Context

The following figure shows the concept of bottleneck analysis.

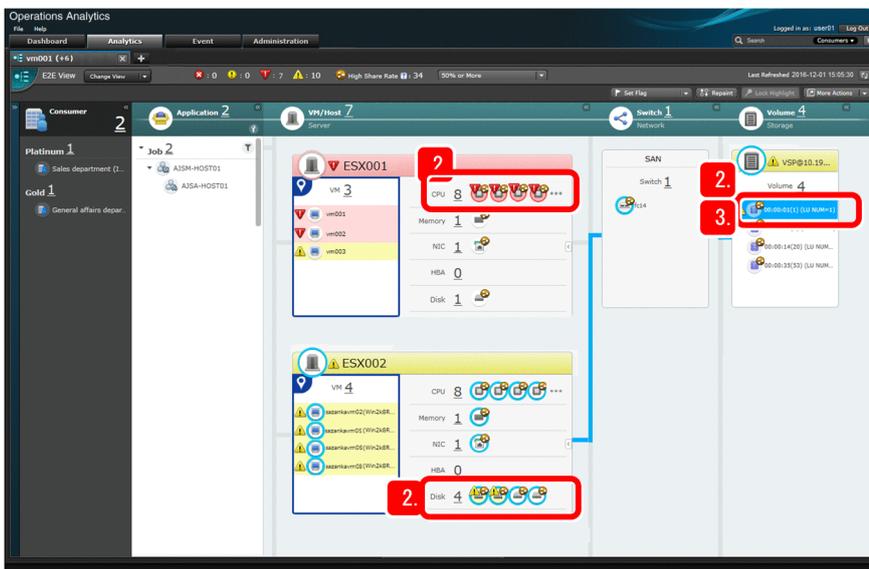


#: Storage components are not monitored by JP1/OA.

The bottleneck analysis starts from the VM on which the error occurred. The bottleneck analyzed here serves as the starting point of the following analyses: the analysis of the importance and scope of the error, which will be performed later, and the analysis of the cause of the error.

Procedure

1. In the **E2E View** window, to get a overview of the business system configuration.
2. The VM in which the error occurred serves as the starting point of the analysis. Check whether there is a warning or error (indicated by a yellow or red icon) in the related components.



Analyze the warnings or errors (indicated by yellow or red icons) that exist in **Disk** and **CPU** of the server, and in **Volume** of the storage system.

3. Click **Volume** of the storage system.
User resources are displayed with their associations to the disk indicated by blue lines.

Inform the storage administrator of the **disk** and **volume** for which a warning is displayed, because the **disk** for which the warning is displayed is associated with the **volume**.

Proceed to the next operation to check whether the **CPU** for which an error is displayed is the bottleneck, because the **CPU** is not associated with storage.

4. To check whether this **CPU** is the bottleneck, click the icon of the **CPU**. Then, from the displayed menu, select **Verify Bottleneck** to open the **Analyze Bottleneck** window.

The **CPU** (bottleneck candidate) appears in a graph in the upper pane, and the **VM** (the **VM** where the problem occurred) appears in a graph in the lower pane.

5. Compare the graph of the **CPU** with the graph of the **VM** to make sure that both graphs indicate the same trend.



If both graphs indicate the same trend, you can determine that the candidate is the bottleneck.

In this example, because the graphs of the **CPU** and **VM** indicate the same trend, you can determine that the **CPU** is the bottleneck.

Tip

In the following cases, assume that the resource displayed in the **E2E View** window with a high sharing rate is the bottleneck, and determine that the resource is the bottleneck in steps 4 and 5:

- When a warning or error (indicated by a yellow or red icon) is not displayed in steps 2 and 3
- When you cannot determine the bottleneck in steps 4 and 5

If you still cannot determine the bottleneck, perform a bottleneck analysis in the **Performance Analysis View** window.

Note

The method for analyzing errors that occur on switches is as follows.

- The cause of the error might be a link-down that was detected when a configuration change results in a port no longer being used. If this is the case, in the detailed window for the switch, use the **Assign Normal** button to change the port status to **Normal**. Doing so will make the port status **Normal** until the status changes again, such as when the port is next used.
- To check the resources related to a specific port, select the target port in the detailed window for the switch, and then click the **Show Related Resources** button. A list of related resources appears. From the list, you can select related resources and then open a new **E2E View** window in which those resources have been set as the base point.

Next steps

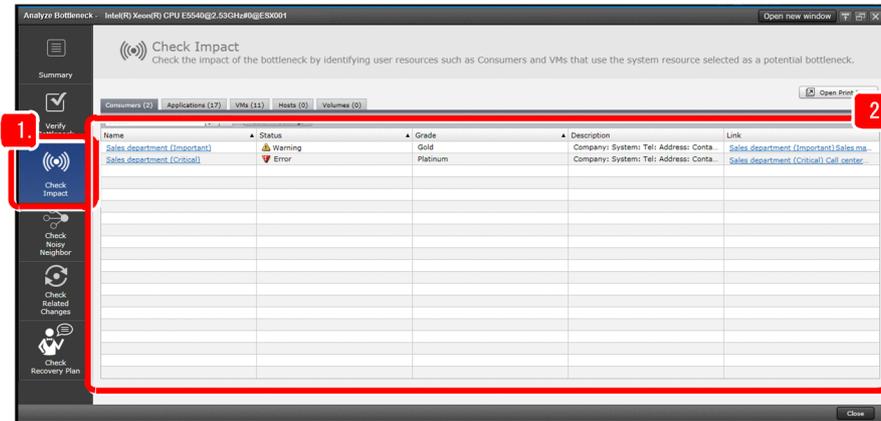
Use the **Analyze Bottleneck** window to analyze the impact and severity of the problem.

3.4 Analyzing the impact and severity of a problem

This section describes how to analyze the impact of the bottleneck and the severity of the problem by using, as the starting point, the CPU that was determined to be the bottleneck. Having understood the impact and severity of the problem, you can then determine the priority of actions to be taken.

Procedure

1. In the **Analyze Bottleneck** window, click **Check Impact**.



The window for analyzing the impact and severity of a problem appears.

2. Based on the displayed **Name** and **Status** of the consumers, you can understand the severity of the problem and its impact on **consumers**.

As needed, change the priority of actions to be taken and initiate contact with consumers who are affected or might become affected by the bottleneck.

Next steps

Analyze the cause of the bottleneck and take action.

Note

You can use JP1/OA to check the impact of the problem location that you reported to the storage administrator.

In this example, click the **volume** that you reported to the storage administrator. Then, from the displayed menu, select **Check Impact** to display the **Analyze Bottleneck** window. In this window, you can check lists of related consumers and virtual machines to understand the impact of the problem location.

If necessary, report the impact of the volume to the storage administrator.

3.5 Analyzing cause and identifying corrective actions

This section describes how to analyze the cause of a bottleneck by using, as the starting point, the CPU determined to be the bottleneck. It also describes how to take corrective actions. The bottleneck might be caused by a consumer's usage of the business system or by changes in the configuration of the IT base system. The manual describes how to analyze causes related to system usage and those related to system configuration changes.

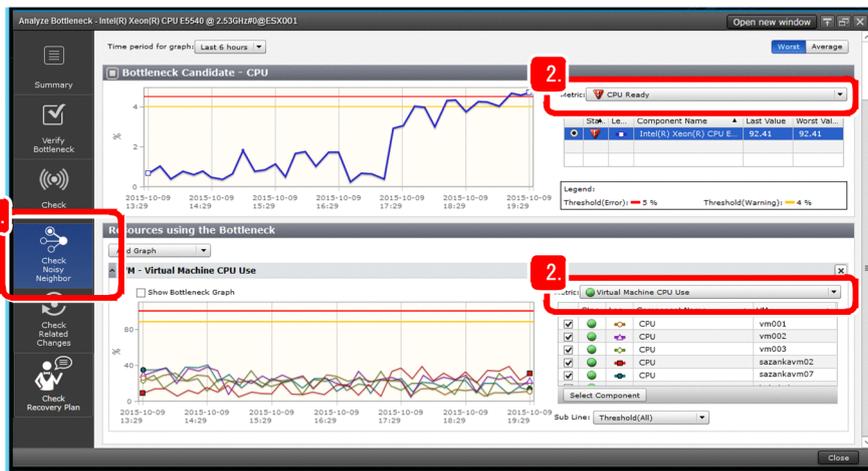
3.5.1 Analyzing the cause

The following describes how to analyze the cause.

(1) Analyzing whether the bottleneck is caused by the usage of the business system

Procedure

1. In the **Analyze Bottleneck** window, click **Check Noisy Neighbor**.



The window for analyzing the cause of a bottleneck appears.

Bottleneck Candidate displays the graph for the **CPU** that was determined to be the bottleneck. **Resources using the Bottleneck** displays the graphs for **VMs**.

2. Select **CPU Ready** from **Metric** of **Bottleneck Candidate**, and then select **Virtual Machine CPU Use** from **Metric** of **Resources using the Bottleneck**. Then, compare the CPU Ready value with the CPU usage to identify the **VM** that is placing a load on the **CPU** of **ESX**.

If the waiting time of the virtual machine was increased at almost the same time as the increase in the CPU usage, there is a problem with the usage of the business system.

3. Look for a graph that has the same shape as the **CPU**.

Because there are no graphs that have the same trend, the usage of the business system did not cause the bottleneck.

Tip

If you cannot determine the cause of the bottleneck from the displayed graphs, check the graphs of different metrics. To view a graph of a different metric, select the metric from **Metric** or add a new

graph by selecting the **Add Graph** menu of **Resources using the Bottleneck**, and then select the metric from **Metric**.

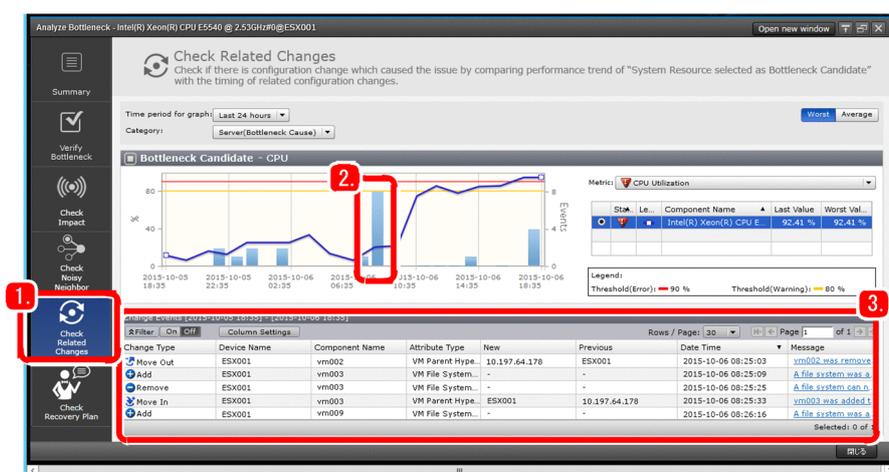
Next steps

Analyze whether the bottleneck was caused by changes in the configuration of the business system.

(2) Analyzing whether the bottleneck is caused by changes in the business system configuration

Procedure

1. In the **Analyze Bottleneck** window, click **Check Related Changes**.



A bar graph indicating the number of events related to changes in the business system configuration, and a line graph for the CPU that was determined to be the bottleneck are displayed.

2. Click the bar graph for the time period before or after the time when the line in the graph for the CPU rises. The table displays previous changes that occurred in the time period shown in the graph as events.
3. Check the details of the events related to changes in the business system configuration in the table. Check whether an event related to changes in the business system configuration affected the bottleneck. By checking the details for the event in which a VM was added, you can determine that the new VM caused the bottleneck.
4. Write down the name of the VM that was added, and then close the **Analyze Bottleneck** window.
5. In the search box in the **Workspace** window, enter the VM name that you checked in step 4.
6. Select **Servers** as the type, and then click **Search**. The VM is displayed.
7. Select the VM.
8. Click **Show E2E View**.

9. Click the icon for the VM. From the displayed menu, select **Show Detail** to check the performance.

Because the performance of the VM affects ESX, ESX can no longer manage the VM. This means that there is a problem in the business system configuration.

Next steps

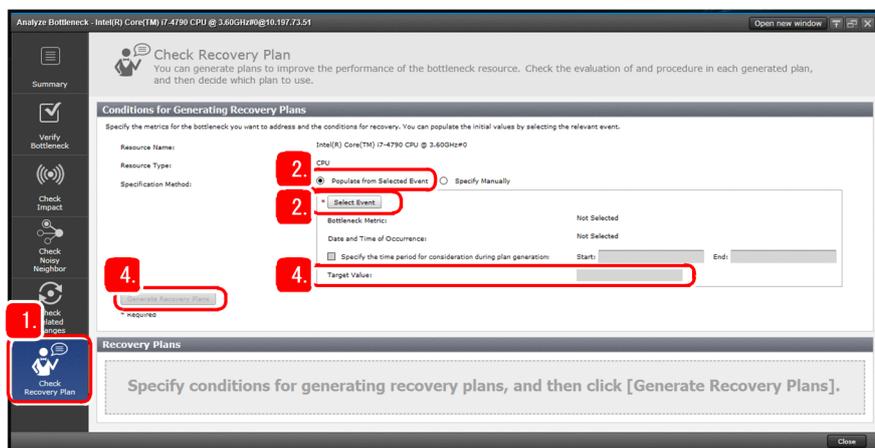
Because you were able to recognize that the addition of a VM caused the bottleneck, give directions to remove the cause.

3.5.2 Removing the cause

The following describes how to remove the cause. JP1/OA can be used to propose recovery plans to improve the performance of system resources based on information related to events and metrics that have caused a bottleneck. You can easily resolve a problem by taking action according to the proposed recovery plans.

Procedure

1. In the **Analyze Bottleneck** window, click **Check Recovery Plan**.



A window for setting the conditions to generate recovery plans appears.

2. In **Specification Method**, make sure that the radio button for **Populate from Selected Event** is selected, and then click **Select Event**.

A window displaying a list of events from which recovery plans are to be created appears.

3. Select the event that caused the bottleneck, and then click **OK**.

In [3.3 Analyzing bottlenecks](#), the CPU was found to be a bottleneck. Search the list and select a warning event related to CPU usage for the entire host.

4. Specify the target value for CPU usage for the entire host in **Target Value** and click the **Generate Recovery Plans** button.

This will display a recovery plan that brings the CPU usage for the entire host close to the target value.

If multiple recovery plans are displayed, compare the details of each plan, and then consider which plan will be effective in resolving the problem.

Note

Depending on the cause of the bottleneck, appropriate recovery plans might not be displayed. In this case, take action based on the cause that you analyzed in the **Analyze Bottleneck** window.

5. Modify the configuration as necessary based on the information provided in the recovery plan.
6. In the **Analyze Bottleneck** window, make sure that all graphs (VM, volumes, and MP) are the same, and that the graphs display a straight line.
If both the line of the graph for the **VM** on which the failure occurred and the line of the graph for the **CPU** of ESX that was determined to be the bottleneck are below the threshold, the problem no longer exists.

Next steps

Inform the persons concerned that the corrective actions for the cause of the bottleneck have been completed.

3.6 Reporting the solution

In this section, you will confirm that the corrective actions for the cause of the problem have been completed and then inform the relevant persons that the problem has been resolved.

Procedure

1. Make sure that the problem has been resolved in [3.5.2 Removing the cause](#), and then contact the appropriate people as shown below:
 - If you recognized the problem via an inquiry from a customer:
Contact the customer who sent the inquiry.
 - If you recognized the problem via contact from an operator:
Contact that operator.
 - If you contacted affected consumers when analyzing the impact and severity of the problem:
Contact the affected consumers again.

This completes the procedure for handling problems.

4

Analyzing problems with an application as the starting point

If a problem occurs in an IT base system that contains applications, by linking JP1/OA with other JP1 products you can analyze the problem from various perspectives such as the time period when the event occurred or the relatedness of the system.

4.1 Workflow for recognizing and resolving problems by using applications as a starting point

The workflow for recognizing and resolving a problem by using an application as a starting point when the application is monitored is as follows:



Note

Even if you are aware of a problem related to an application based on a notification from a customer or operator, if you have not received a JP1 event notification, you will not be able to identify the problem by using the procedure described in this chapter. In such cases, in the **E2E View** window, check the elements that make up the IT base system and are related to the application, and then perform bottleneck analysis.

| # | Workflow |
|--|---|
| 1 | 4.2 Recognizing a problem from a JP1/IM event notification |
| 2 | 4.3 Analyzing events to identify the configuration element that has a problem |
| After identifying the cause of the problem by event analysis, perform the following bottleneck analysis steps, which are described in Chapter 3. | |
| 3 | 3.3 Analyzing bottlenecks |
| 4 | 3.4 Analyzing the impact and severity of a problem |
| 5 | 3.5 Analyzing cause and identifying corrective actions |
| 6 | 3.6 Reporting the solution |

4.2 Recognizing a problem from a JP1/IM event notification

By examining the JP1 events issued by JP1/IM, you can recognize problems in applications. If you cannot resolve a problem by following the event messages, analyze the event details to identify the cause of the problem. This manual describes the general procedure for recognizing that an application in JP1/OA has a problem, based on the events issued by JP1/IM.

Before you begin

The following is an example in which an event corresponding to abnormal termination of a jobnet was issued in JP1/AJS3 - Manager.

Procedure

1. Check the content of the event issued by JP1/IM, and identify the application that you think has a problem.
In this manual, from the content of the notification event, it is assumed that an application related to JP1/AJS3 - Manager (the application name is AJSM-HOST01) has a problem.
2. To start analyzing the application, log in to JP1/OA.
3. Click the **Analytics** tab.
4. In the text box of the **Analytics** window, enter the application name that you think has a problem.
5. From the pull-down menu for the type, select **Application**, and then click **Search**.
Applicable applications are displayed as search results.
6. From the search results, select the application to analyze.
By referring to the displayed information (such as the application name, application type, and consumer name), verify that the application is the one to be analyzed.
7. Click **Show E2E View**.
The **E2E View** window displays the configuration elements of the IT base system related to the selected application.
8. In the **E2E View** window, verify the location of the problem.



Note

By linking with JP1/IM, you can directly call JP1/OA windows from JP1 events. For details, see [A. Using the product more efficiently](#).

Next steps

In the **E2E View** window, analyze the events to identify the configuration element that you think has a problem.

4.3 Analyzing events to identify the configuration element that has a problem

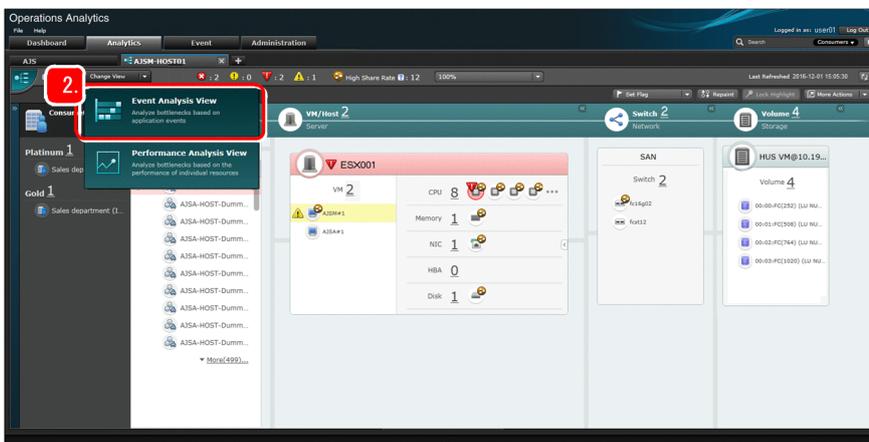
From the JP1 events that occurred in an application, analyze the performance of the related system configuration elements, and identify the configuration element that has a problem. Events that occurred in the application are sorted chronologically by JP1/OA and are sorted according to the relationships between the applications. From the sorted events, check the details of the events starting with those that have the highest probability of containing the cause of the problem, and filter the events to be analyzed. Then, analyze the filtered events and the resource performance trends related to these events to identify which configuration elements have a problem.

Procedure

1. In the **E2E View** window, understand the configuration of the IT base system.

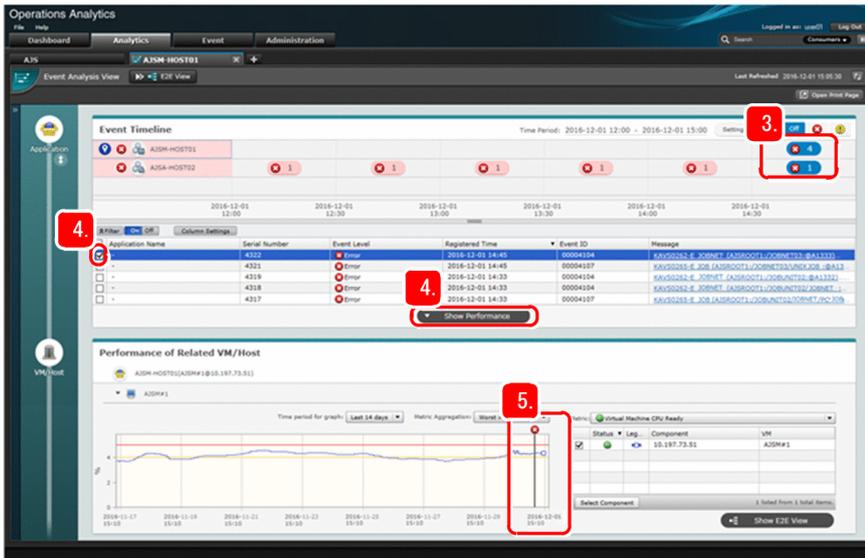
You can check elements related to the application that was selected as the starting point, as well as the status of occurrence of warnings and errors.

2. To check events that are occurring in the application, click the **Event Analysis View** button.



Events that occurred in the related application and the application that was selected as the starting point are displayed in chronological order. The most recent events that have a greater probability of affecting the application are displayed in the upper-right corner of the window.

- In the next window, you can check multiple events that occurred during the last 30 minutes in the starting-point application AJSM-HOST01 and the highly relevant application AJSA-HOST02 most recently around the same time. To analyze these events, click the event button.



Detailed information such as messages and the time when events occurred is displayed.

- To analyze the resource performance status at the time that an event occurred, select an event to analyze from the displayed event list, and then click the **Show Performance** button.

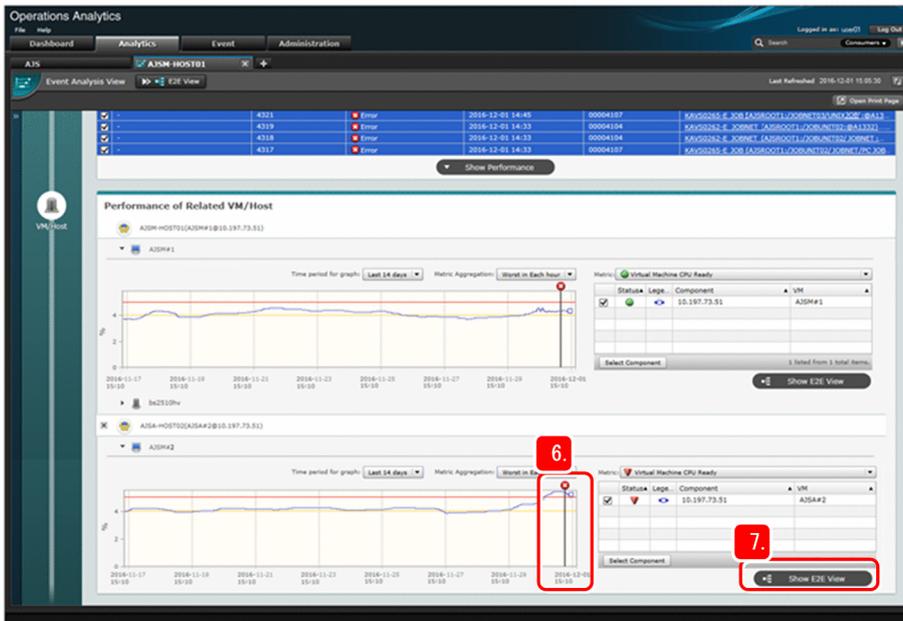
Detailed information for the most recent events is displayed at the top, enabling you to check performance information from the top one by one.

If you click the **Show Performance** button, the performance graphs and metric information for virtual machines or hosts (considered virtual machines in this manual) related to the selected events will be displayed. If the related resources are virtual machines, information about the hypervisors on which the virtual machines are running will also be displayed.

- Check the selected event and virtual machine performance trends.

In the displayed performance graph, you can see that there were no notable changes in the performance of the virtual machine of AJSM-HOST01 when the event occurred. The second, third, and fourth events are also related to AJSM-HOST01, which indicates that these events are not relevant to the virtual machine performance trends either.

6. Select the event in AJSA-HOST02, and click the **Show Performance** button to check the virtual machine performance of AJSA-HOST02.



In the performance graph for the virtual machine of AJSA-HOST02, you can see that performance degraded significantly just before the event occurred. From this you can conclude that the virtual machine of AJSA-HOST02 is causing the problem in the starting-point application.



Tip

In the **Event Analysis View** window, you can sometimes identify the cause by checking both the performance graph for virtual machines and the performance graph for hypervisors. If there is no problem related to virtual machines or hypervisors, you can assume that applications are the cause of the problem.

7. To continue with an analysis of the virtual machine of AJSA-HOST02, click the **Show E2E View** button.

Next steps

In the **E2E View** window that uses the virtual machine of AJSA-HOST02 as a base point, analyze bottlenecks.

5

Analyzing problems by analyzing correlations in performance data

If you cannot identify a target of analysis even after checking the **E2E View** window or in the **Event Analysis View** window, for example, because the status of the IT base system has not changed, use the **Performance Analysis View** window to analyze correlations in performance data and to find latent problems.

5.1 Workflow for analyzing problems by analyzing correlations in performance data

The workflow for analyzing problems by analyzing correlations in performance data is as follows:

| # | Workflow |
|---|--|
| 1 | 5.2 Analyzing problems by analyzing correlations in performance data |
| After analyzing correlations in performance data, perform the procedure for analyzing the impact and severity of a problem, as well as the procedures listed below it. These procedures are described in chapter 3. | |
| 2 | 3.4 Analyzing the impact and severity of a problem |
| 3 | 3.5 Analyzing cause and identifying corrective actions |
| 4 | 3.6 Reporting the solution |

5.2 Analyzing problems by analyzing correlations in performance data

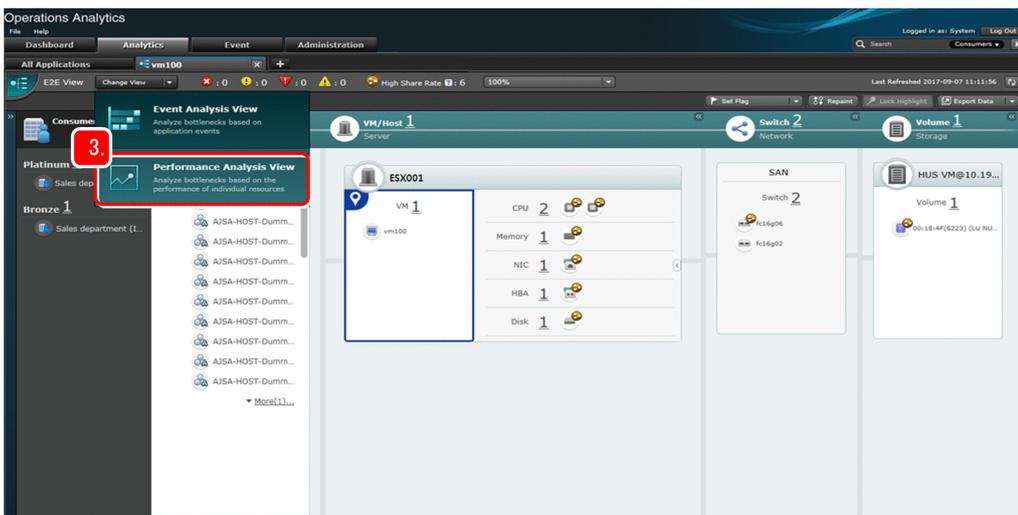
Identify the cause of a problem by analyzing correlations in performance data. This method is useful when you cannot identify a problem with the system, for example, because the status of the IT base system has not changed. This manual first describes how to identify the targets of analysis based on the performance data of each resource, and then describes how to analyze the cause of a problem.

Before you begin

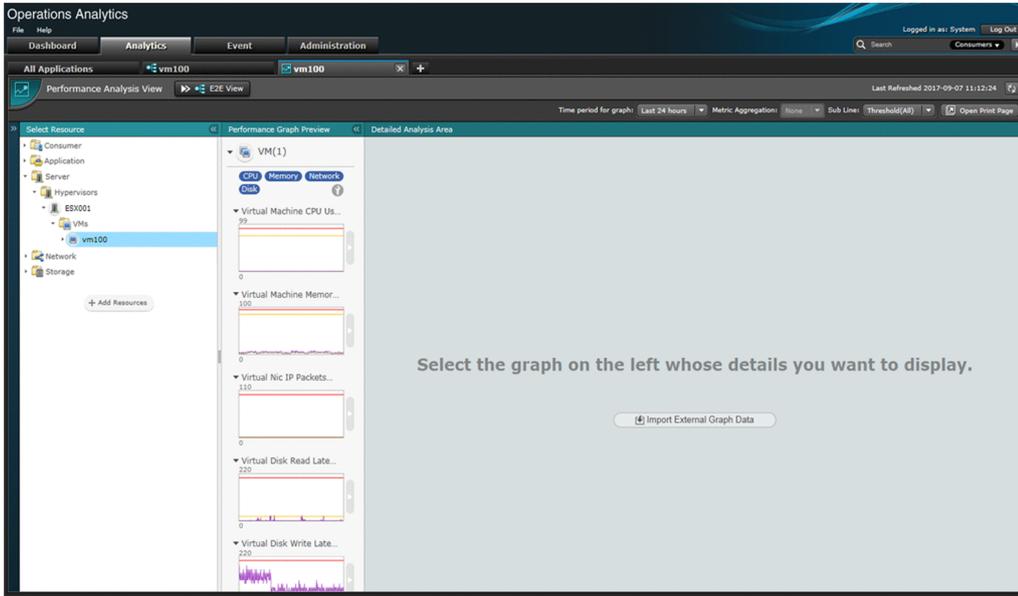
The examples in the procedure below assume the following context: An administrator receives a notification from a customer that a particular application was slow. The administrator checks the information in the **E2E View** window and the **Event Analysis View** window, but could not find any resource whose status indicates the occurrence of a warning or an error. Thus, the administrator could not identify the problem.

Procedure

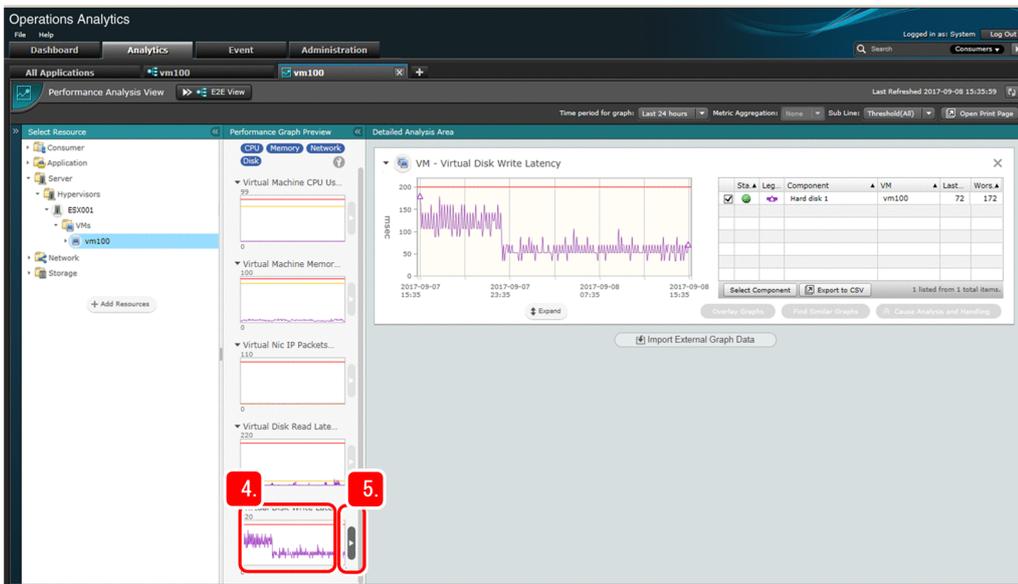
1. Change the base point of the analysis to the virtual machine on which the application is running, and then open the **E2E View** window.
2. Check the configuration information of devices related to the virtual machine.
The problem cannot be identified, because there are no resources whose statuses indicate the occurrence of a warning or an error.
3. Click the **Performance Analysis View** button to analyze the problem by analyzing correlations in performance data.



In the **Select Resource** area of the **Performance Analysis View** window, configuration information about devices related to the virtual machine that was used as the base point of analysis is displayed. Performance graphs of the main metrics of the virtual machine are displayed in the **Performance Graph Preview** area.



4. In the **Performance Graph Preview** area, check the lines in the performance graphs of the virtual machine. Look for a graph that might indicate the cause of the problem.



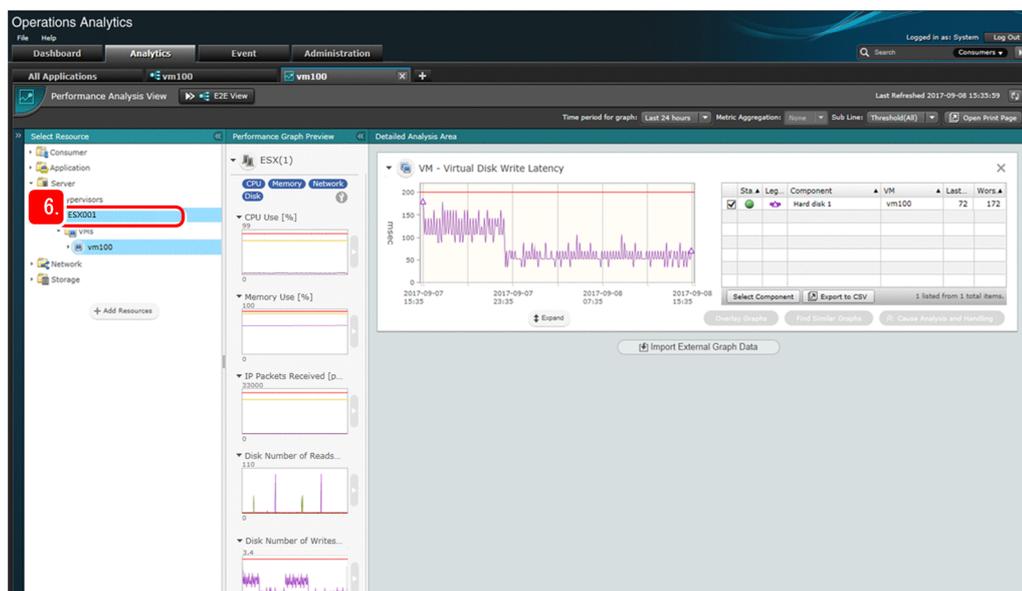
5. To check the details of a graph, click the arrow on the right to enlarge the graph in the **Detailed Analysis Area** area. The enlarged graph indicates that the performance of virtual machine vm100 with respect to the **Virtual Disk Write Latency** metric seems to have deteriorated at a certain time period in the past. You can use the enlarged graph in the **Detailed Analysis Area** in operations (such as overlaying graphs and searching for similar graphs) for the purpose of analysis.

Note

You can compare performance graphs in JP1/OA against performance information managed by other software (such as data in JP1/PFM reports) to see whether there are any correlations. To do so, import the information output by the other software. The information can be used in the same ways that performance information from JP1/OA can be used: for example, in overlaying graphs or searching for similar graphs.

For details about the types of external data that can be imported, see the *JPI/Operations Analytics Configuration and Administration Guide*.

- To start analysis, from the **Select Resource** area, select the hypervisor ESX001 on which virtual machine vm100 is running.



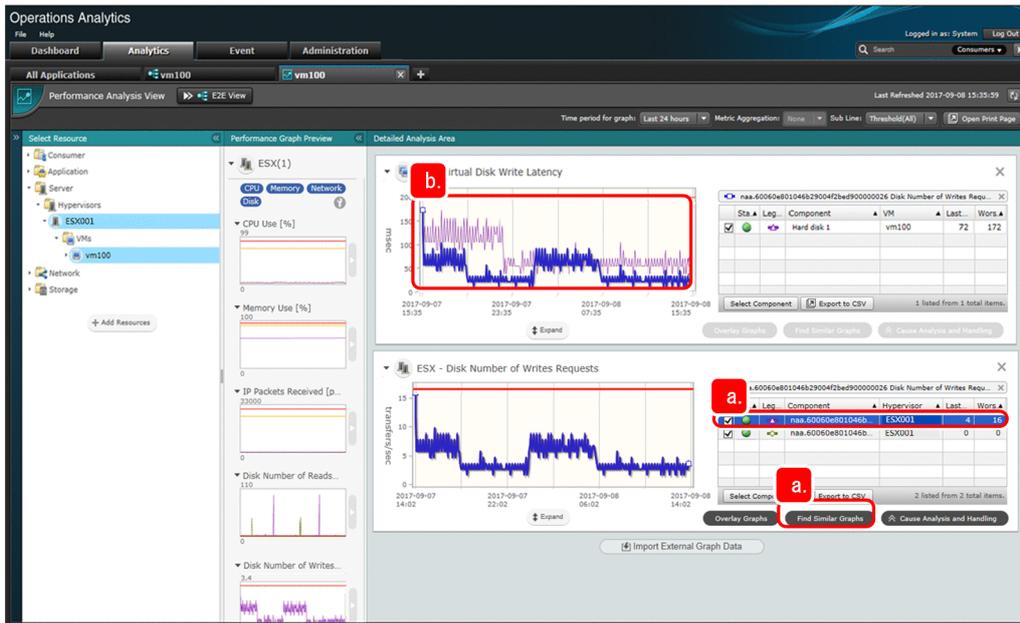
In the **Performance Graph Preview** area, the performance graphs of the main metrics of hypervisor ESX001 are also displayed.

- In the performance graphs of hypervisor A, look for a metric that might be related to the metric of the comparison source.

The **Disk Number of Writes Requests** metric of hypervisor is of the same type as the **Virtual Disk Write Latency** metric of virtual machine. Enlarge the graph of the **Disk Number of Writes Requests** metric of hypervisor in the **Detailed Analysis Area** area for further analysis.

8. In the **Detailed Analysis Area** area, compare the lines in the enlarged graphs by overlaying one graph on top of the other.

a. Of the graphs of hypervisor ESX001, select a graph that shows changes, and then click the **Overlay the Graph** button.



The graph of hypervisor is overlaid with the graph of virtual machine.

b. Check the overlaid graphs.

Although the lines of the overlaid graphs look similar for a certain period of time, this alone is still insufficient to determine that the problem is caused by **Disk Number of Writes Requests** of hypervisor ESX001.

9. Repeat steps 7 and 8 for other metrics that might be relevant until you find the bottleneck.

Because the cause of the problem cannot be identified even after investigating other relevant metrics, the scope of the investigation is expanded to include all virtual machines running on hypervisor ESX001.

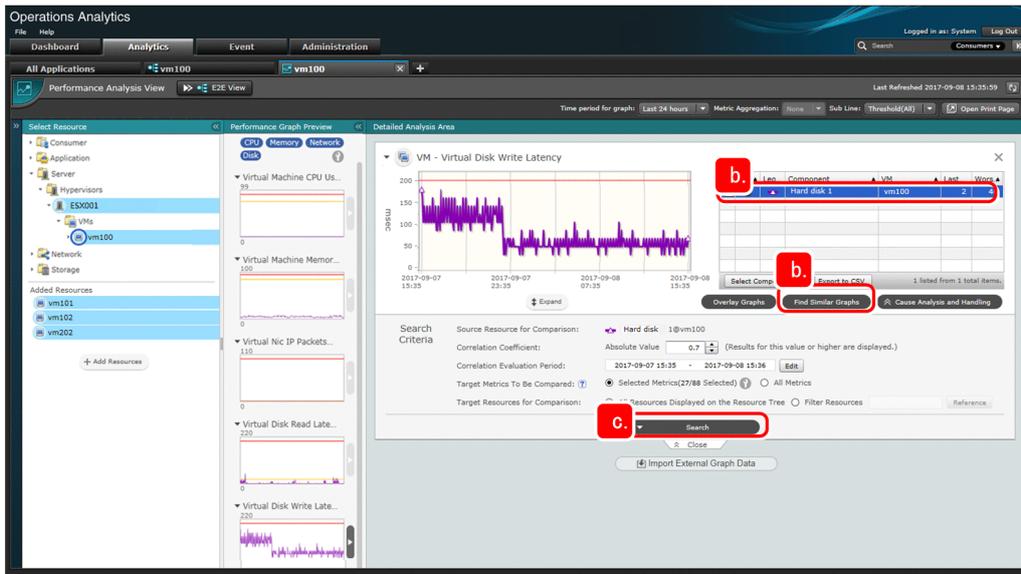
However, because the **Select Resource** area displays only resources that are related to virtual machine (which was used as the base point of analysis), it will take time to check all virtual machines by repeatedly overlaying their graphs. For this reason, use correlations in performance data to search for performance graphs.

10. Search for graphs that are similar to the graph of virtual machine vm100.

a. To include all virtual machines on hypervisor within the scope of the search, add the applicable virtual machines to the **Select Resource** area.

Click the **Add Resources** button and add the virtual machines required for the search.

b. Select the graph of virtual machine vm100 and click the **Find Similar Graphs** button.



The search conditions to be set are displayed.

c. Set the search conditions, and then click the **Search** button.

Tip

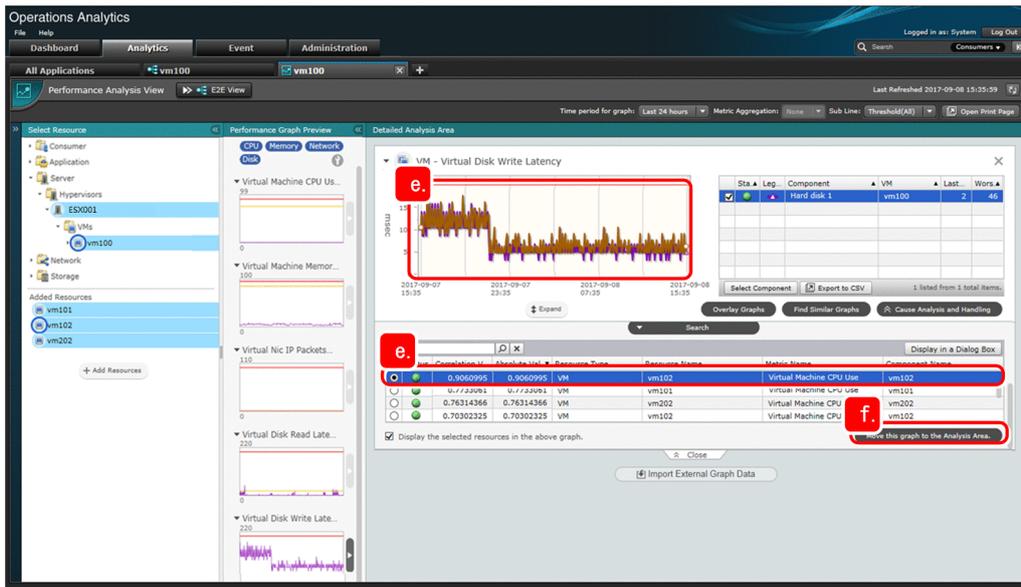
The correlation coefficient is a value that indicates the degree of correlation between two lines in a graph. A coefficient close to 1 indicates a strong positive correlation between the lines, whereas a coefficient close to -1 indicates a strong negative correlation between the lines (the lines have opposing trends). Specify this search condition as an absolute value. Metrics for which the absolute value of the correlation coefficient is equal to or greater than the specified value will be returned as search results.

The default value is 0.7 . In this case, metrics for which the absolute value of the correlation coefficient is equal to or greater than 0.7 (in other words, in the range from -1.0 to -0.7 or in the range from 0.7 to 1.0) will be returned as search results.

d. The search results are displayed as a list of resource metrics in descending order of the absolute values of the correlation coefficient.

The list includes the **CPU Use** metric of virtual machine vm102.

- e. Select each metric, in descending order of the absolute values of the correlation coefficient, and then check whether the lines in the graph of the metric are similar to those in the graph of virtual machine vm100 (the comparison source).

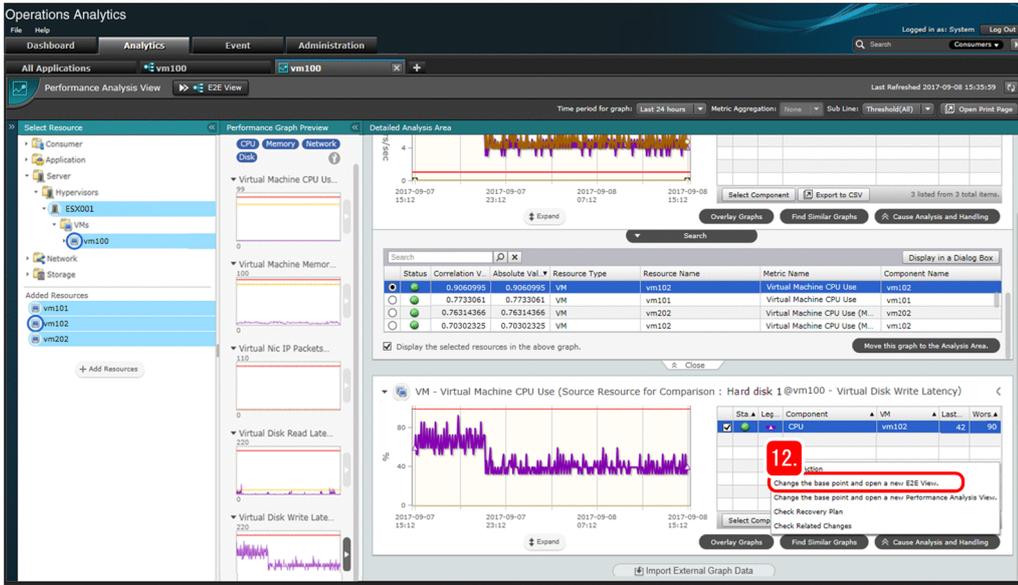


When the **CPU Use** metric of virtual machine vm102 is selected in the list, the graph of the selected metric is displayed, overlaid with the comparison-source graph. By examining the overlaid graphs, you can see that the two graphs are very similar. As a result, this metric can be identified as a possible cause of the problem.

Note

Despite the high value of the correlation coefficient, the comparison-source graph and the compared graph sometimes do not appear to be correlated. This is because the graphs are displayed differently depending on the metric units.

- f. If you want to find other similar graphs by checking other metrics in the list of search results, for the time being, click the **Move this graph to the Analysis Area** button. The graph will be enlarged and displayed in the **Detailed Analysis Area** area.
11. Repeat the previous steps for other metrics, in descending order of the absolute values of the correlation coefficient, and check for similar graphs until you have narrowed down the possible causes of the problem. The graph of the **CPU Use** metric of virtual machine vm102 is most similar to the comparison-source graph. Based on this result, virtual machine vm102 is identified as the cause of the problem.
 12. Continue to analyze the problem of virtual machine vm102. From among the graphs that are displayed in the **Detailed Analysis Area** area, select the graph of the **CPU Use** metric of virtual machine vm102, and then click the **Change the base point and open a new E2E View** button.



The **E2E View** window appears and virtual machine vm102 is set as the base point.



Tip

For a small-scale business system, you can analyze the cause of the problem by continuing the analysis in the **Performance Analysis View** window. To continue the analysis, click the **Change the base point and open a new Performance Analysis View** button.

Next steps

Check the configuration information in the **E2E View** window, where virtual machine vm102 is set as the base point of analysis, and then continue to analyze the impact and severity of the problem.

Appendixes

A. Using the product more efficiently

This section explains how to use JP1/OA more efficiently. For details, see the *JP1/Operations Analytics Configuration and Administration Guide*.

Monitoring resources by using SNMP traps

You can register received SNMP traps as events in JP1/OA. In addition, you can also register the sources that issue traps as management targets in JP1/OA. This enables you to quickly grasp any changes in the state of your IT resources.

Managing user accounts by using the authentication function of JP1/Base

You can use the authentication function of JP1/Base to manage user accounts of JP1/OA. By linking with JP1/Base, you will not need to manage users in JP1/OA. You can also use JP1 users that were already created.

Analyzing the cause of a failure based on JP1 event information

You can select a JP1 event from a JP1/IM window to start a window of JP1/OA. The administrator can analyze the cause of a failure by checking the node related to the JP1 event information.

Issuance of JP1 events

Events to be registered in the **Event** tab of JP1/OA can be issued as JP1 events.

Registering a change management item

By linking with JP1/Service Support, you can use JP1/OA to register an action to be taken for a failure in JP1/Service Support as a change management item. By managing actions as items, you can visualize the workflow and share information among persons in charge to proceed with operations.

Instructing the operator to take action for a failure

By linking with JP1/Navigation Platform, you can use JP1/OA to instruct the operator to take action for a failure. The operator can take action for the failure while using a JP1/Navigation Platform window to check how to take action.

Expanding the management targets

In JP1/OA, the following resources can also be managed, in addition to the management targets described in this manual. By expanding the management targets, you can easily understand the status of a diversified IT platform system.

- Applications (including third-party products)
- Containers
- Cloud environments
- Hosts or storage systems of your choice (via SNMP)

B. Version Changes

B.1 Changes in version 12-60

- Microsoft Edge is now supported.
- The **Show Related Resources** button was added, and the **E2E View** window can now be opened from the list of resources associated with a specific port on a switch.

B.2 Changes in version 12-50

- Google Chrome is now supported.
- It is now possible to manage cloud environments.

B.3 Changes in version 12-10

- Windows Server 2019 is now supported.
- **Perform Alive Monitoring** was added to the IP address range settings. You can now perform alive monitoring even if you do not specify credentials.
- You can now register received SNMP traps as events or management targets in JP1/OA.
- JP1 events can now be issued.
- Container monitoring is now available.

B.4 Changes in version 12-00

- Supported Firefox versions were changed.
- By registering a plug-in, you can now monitor resources that use the SNMP protocol. The relevant descriptions were added accordingly.

B.5 Changes in version 11-50

- You can now analyze problems by analyzing correlations in performance data. The relevant descriptions and screenshots were added or changed accordingly.
- Supported Firefox versions were changed.
- **Classification Label** was added as an item to be set for the IP address range. This item allows hosts to be displayed in groups in the **E2E View** window. The relevant descriptions and screenshots were added or changed accordingly.
- When performance information about virtual machines is displayed in the **Event Analysis View** window, performance information about the hypervisors on which the virtual machines are running is now also displayed. The relevant descriptions and screenshots were added or changed accordingly.
- Applications such as third party products can now be monitored. The relevant descriptions were added accordingly.

B.6 Changes in version 11-10

- Windows Server 2016 is now supported.
- By linking JP1/OA with other JP1 products, the status of the IT base system, including applications, can now be monitored, and problems can now be analyzed. Related descriptions were added or modified accordingly.
- Supported Firefox versions were changed.
- The FC switch can now be monitored by using the SNMP protocol. Related descriptions were modified accordingly.
- The following content about the management functionality of consumers was added or modified:
 - *Example of associating devices with users* was changed so the device to be managed is associated with multiple consumers.
 - Steps for entering a URL and its display name, such as for web systems, were added to the procedure for creating consumers.
- A description was added for functionality that assumes the port status of the switch is normal.
- A recovery plan to improve the performance of system resources can now be proposed from JP1/OA. The procedure for resolving the causes of bottlenecks was modified accordingly.

C. Reference material for this manual

This section provides reference information, including various conventions, for this manual.

C.1 Related publications

This manual is part of a related set of manuals. The manuals and manual numbers in the set are listed below.

- JP1/Operations Analytics Configuration and Administration Guide (3021-3-D61(E))
- JP1/Operations Analytics Messages (3021-3-D62(E))
- JP1/Operations Analytics REST API Reference Guide (3021-3-D63(E))

C.2 Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

| Abbreviation | Full name or meaning |
|------------------------|---|
| Hyper-V | Microsoft(R) Windows Server(R) 2012 Hyper-V(R) |
| | Microsoft(R) Windows Server(R) 2012 R2 Hyper-V(R) |
| | Microsoft(R) Windows Server(R) 2016 Hyper-V(R) |
| | Microsoft(R) Windows Server(R) 2019 Hyper-V(R) |
| Internet Explorer | Windows(R) Internet Explorer(R) |
| Windows Server 2012 | Microsoft(R) Windows Server(R) 2012 Datacenter |
| | Microsoft(R) Windows Server(R) 2012 Standard |
| Windows Server 2012 R2 | Microsoft(R) Windows Server(R) 2012 R2 Datacenter |
| | Microsoft(R) Windows Server(R) 2012 R2 Standard |
| Windows Server 2016 | Microsoft(R) Windows Server(R) 2016 Datacenter |
| | Microsoft(R) Windows Server(R) 2016 Standard |
| Windows Server 2019 | Microsoft(R) Windows Server(R) 2019 Datacenter |
| | Microsoft(R) Windows Server(R) 2019 Standard |

Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012 are sometimes collectively abbreviated as "Windows".

C.3 Conventions: Fonts and symbols

The following table explains the text formatting conventions used in this manual:

| Text formatting | Convention |
|-----------------|--|
| Bold | <p>Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example:</p> <ul style="list-style-type: none"> From the File menu, choose Open. Click the Cancel button. In the Enter name entry box, type your name. |
| <i>Italic</i> | <p>Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none"> Write the command as follows: <code>copy source-file target-file</code> The following message appears: A file was not found. (file = <i>file-name</i>) Italic characters are also used for emphasis. For example: Do <i>not</i> delete the configuration file. |
| Monospace | <p>Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none"> At the prompt, enter <code>dir</code>. Use the <code>send</code> command to send mail. The following message is displayed: <code>The password is incorrect.</code> |

The following table explains the symbols used in this manual:

| Symbol | Convention |
|--------|---|
| | In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: <code>A B C</code> means A, or B, or C. |
| { } | In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: <code>{ A B C }</code> means only one of A, or B, or C. |
| [] | In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: <code>[A]</code> means that you can specify A or nothing. <code>[B C]</code> means that you can specify B, or C, or nothing. |
| ... | In coding, an ellipsis (...) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: <code>A, B, B, ...</code> means that, after you specify A, B, you can specify B as many times as necessary. |

C.4 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names.

| Abbreviation | Full name or meaning |
|--------------|---------------------------------------|
| ESX | VMware vSphere(R) ESXi(TM) |
| JP1/AJS3 | JP1/Automatic Job Management System 3 |
| JP1/IM | JP1/Integrated Management |
| | JP1/Integrated Management 2 |

| Abbreviation | Full name or meaning |
|--------------|----------------------------|
| JP1/OA | JP1/Operations Analytics |
| JP1/PFM | JP1/Performance Management |
| VMware | VMware(R) |

C.5 Conventions: Acronyms

This manual uses the following acronyms.

| Acronym | Full name or meaning |
|---------|---|
| FC | Fibre Channel |
| SMI-S | Storage Management Initiative - Specification |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| WBEM | Web-Based Enterprise Management |
| WMI | Windows Management Instrumentation |

C.6 Conventions: KB, MB, GB, and TB

This manual uses the following conventions: 1 KB (kilobyte) is 1,024 bytes, 1 MB (megabyte) is 1,024² bytes, 1 GB (gigabyte) is 1,024³ bytes, and 1 TB (terabyte) is 1,024⁴ bytes.

Index

A

- Analyzing and resolving problems 40
- Analyzing bottlenecks 45
- Analyzing cause and identifying corrective actions 49
- Analyzing events to identify the configuration element that has a problem 57
- Analyzing problems by analyzing correlations in performance data 62
- Analyzing the cause 49
- Analyzing the impact and severity of a problem 48
- Analyzing whether the bottleneck is caused by changes in the business system configuration 50
- Analyzing whether the bottleneck is caused by the usage of the business system 49
- Associating devices with users 32

C

- Configuring device monitoring 35
- Configuring email notification 38
- Configuring JP1/OA 23
- Configuring the mail server 24
- Creating a user account 23

D

- Device configuration 26

I

- Installation and configuration 17
- Installation prerequisites 19
- Installing JP1/OA 21

L

- Logging in to JP1/OA 22

O

- Overview 10

R

- Reading this manual 15
- Recognizing a problem from a JP1/IM event notification 56
- Recognizing problems by using JP1/OA 42
- Recognizing problems from notifications from a customer or operator 43

Recognizing the problem and identifying the target of the analysis 42

Registering devices using the discovery method 29

Registering JP1 products to be managed using the management tool registration method 31

Registering management targets 26

Registering vCenter systems using the management tool registration method 28

Removing the cause 51

Reporting the solution 53

S

Setting monitoring conditions for system resources 37

Setting monitoring conditions for user resources 36

Setting the collection intervals 35

W

What is explained in this manual 13

What you can do with JP1/OA 11

Workflow for analyzing problems by analyzing correlations in performance data 61

Workflow for installation and configuration 18

Workflow for recognizing and resolving problems 41

Workflow for recognizing and resolving problems by using applications as a starting point 55

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
