CA92344-2540-02

FUJITSU Software Infrastructure Manager V2.3
Infrastructure Manager for PRIMEFLEX V2.3
Operating Procedures for Packet Analysis of Virtual Network

October 2018

FUJITSU LIMITED

Modification History		
Edition	**Publication Date**	**Modification Overview**
01	August 2018	First Edition
02	October 2018	2.2.1 Obtaining Analysis VM: Added a table for supported ISM version and Analysis VM 2.5 Traffic Check: Added image for ISM 2.3.0.b or later 2.6 Packet Analysis: Added parameters and descriptions for Analysis VM Deploy Settings (vCenter) of ISM 2.3.0.b or later 2.6.3 Analysis Status Check: Added actions for error message of ISM 2.3.0.b or later

This document provides information on operating procedures for Packet Analysis of Virtual Network in FUJITSU Software Infrastructure Manager V2.3 and FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.3.

"Infrastructure Manager for PRIMEFLEX" is available only in Japan, APAC, and North America.

Hereinafter, "Infrastructure Manager" is referred to as "ISM", and "Infrastructure Manager for PRIMEFLEX" is referred to as "ISM for PRIMEFLEX." When description is provided without distinguishing "Infrastructure Manager" from "Infrastructure Manager for PRIMEFLEX", it is referred to as "Infrastructure Manager" or "ISM" as a unified description.

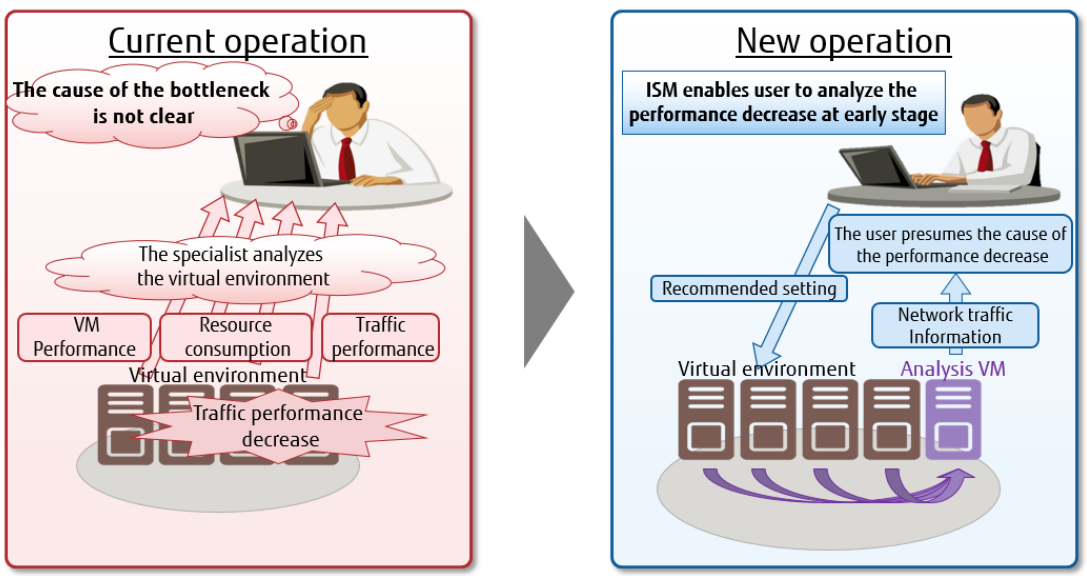
For the details and abbreviations used in this document, refer to the manuals for ISM or ISM for PRIMEFLEX listed below.

- User's Manual
- Glossary
- Settings for Monitoring Target OS and Cloud Management Software

1. Overview of Packet Analysis of Virtual Network

1.1. Overview of Function

This function displays the trends of the traffic volume and the status of the traffic quality by port, by network, or by host based on the collected packet information. With this information, users can grasp the network trend and identify any trouble smoothly by themselves.



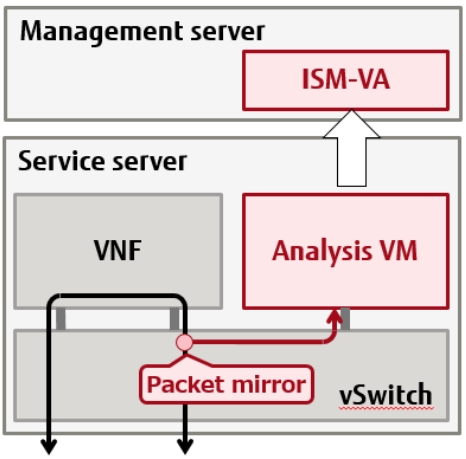
1.2. Structure

Analysis VM is deployed on the host OS where traffic performance is decreasing. Analysis VM captures and analyzes the actual packet flowing over the virtual switch to calculate the following performance information.

- Performance information by port number (TCP/UDP), by terminal (VM), or by session.
- Quality degradation information such as traffic volume, the number of packet loss, or the volume of traffic delay.

Point

- Analysis VM only analyzes the captured header information of the packet (L2, L3, L4 headers).
- After analyzing the header information, the captured header information is discarded without being saved, meaning that no information is saved.



1.3. Display Item

The function displays the following information.

I. Statistical performance information on the monitoring targets (host OS, virtual OS, or virtual network adapter)

Display Item	Description
CPU usage	Displays the utilization rate of the physical CPU on the target host.
CPU usage of VM vCPU	Displays the utilization rate of the virtual CPUs for each virtual machine operating on the target host.
CPU usage of virtual network adapter	Displays the CPU utilization rate in virtual network adapter units.
Traffic information of virtual network adapter	Displays the volume of the sent and received packets, the number of error packets, and the number of dropped packets for each virtual network adapter.

II. Packet analysis results showing information on details and quality of communication

Monitoring Targets of Analysis VM	Description
Port traffic information	Displays the sent and received packet information for each TCP/UDP port.
Network traffic information	Displays the sent and received packet information for each subnet.
Host traffic information	Displays the sent and received packet information for each host.
Host quality information	Displays the communication quality of the TCP (number of losses, delay time, etc.) for each host.

1.4. System Requirements

To use Packet Analysis of Virtual Network, check the following resources in advance because they are additionally required.

For the system requirements for virtual machines operated by ISM-VA, refer to the "1.5.1 System Requirements for ISM-VA (Virtual Machines)" in "User's Manual."

・ System Requirements for ISM-VA(Virtual Machines)

Number of nodes	Number of CPU cores	Memory capacity	Disk capacity
1 to 100	4 cores or more	16 GB or more	85 GB or more
101 to 400	6 cores or more	16 GB or more	160 GB or more
401 to 1000	10 cores or more	20 GB or more	310 GB or more

・ System Requirements for Host Operated by Analysis VM

Number of CPU cores	Memory capacity	Disk capacity
2 cores or more	4 GB or more	20 GB or more

Note

- The upper limit of virtual adapter that can be monitored by the function is 1000.
- The upper limit of simultaneous analysis using Analysis VM is 10.
- The monitored data will be stored for up to 30 days, and the obsolete one will be deleted.
- The monitored data of Analysis VM will be deleted when Analysis VM is deleted.

1.5. Support Target

1.5.1. OS and Cloud Management Software to be supported

OS and Cloud Management Software that Packet Analysis of Virtual Network can be used for are as follows.

[OS]

VMware :

Esxi 5.5 / 6.0 / 6.5 / 6.7

Linux：
Redhat Enterprise Linux 7.2 / 7.3 / 7.4 / 7.5

[Cloud Management Software]
VMware：
vCenter Server 5.5 / 6.0 / 6.5 / 6.7
vCSA 5.5 / 6.0 / 6.5 / 6.7

Linux:
OpenStack (Red Hat Enterprise Linux)

Note

- To monitor the virtual network adapter, some settings may be required for OS or Cloud Management Software to be used in advance.
- For operational performance using OpenStack, contact your local Fujitsu customer service partner.

For a method to set OS or Cloud Management Software to be monitored, refer to "Settings for Monitoring Target OS and Cloud Management Software."

1.5.2. The Number of Monitoring Target

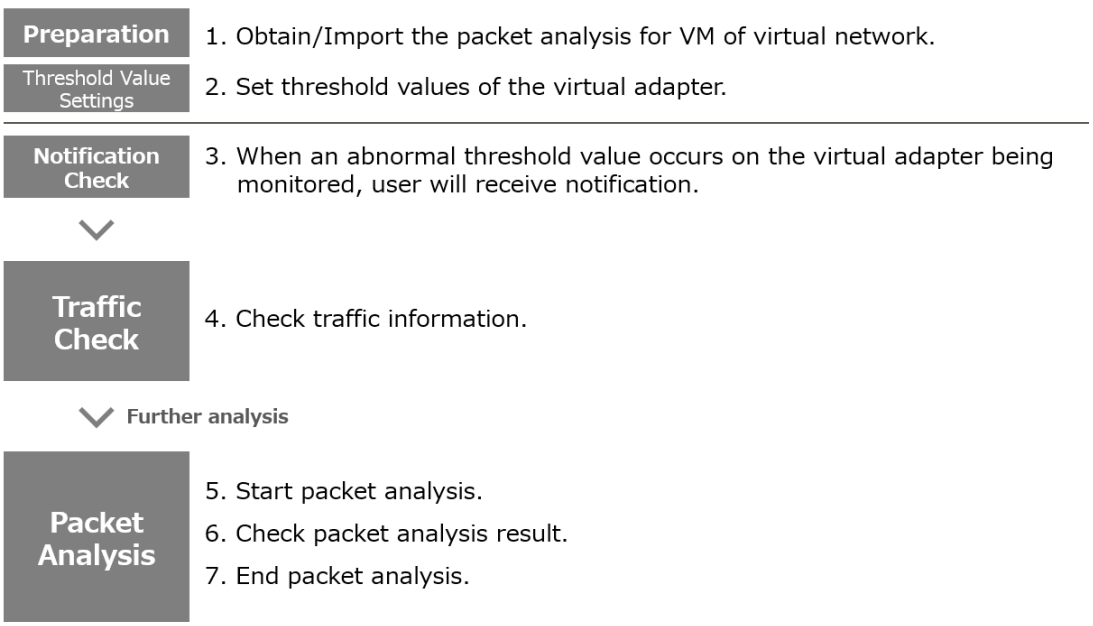
Maximum 1000 virtual adapters

1.5.3. Data Retention Time

Within 1 month

2. Procedure for Operating Packet Analysis of Virtual Network

2.1. Overview



2.2. Preparation

2.2.1. Obtaining Analysis VM

- Table for supported ISM version and Analysis VM

ISM version	Infrastructure Manager Analysis VM for KVM	Infrastructure Manager Analysis VM for VMware
ISM 2.3.0	V1.0.0	V1.0.0
ISM 2.3.0.b	V1.1.0	V1.1.0

To obtain Analysis VM of virtual network, contact your local Fujitsu service partner.

2.2.2. Importing Analysis VM

Deploy a VM image on ISM-VA.

Deploy the VM image in the file transferring area "/Administrator/ftp" within ISM-VA using FTP client.

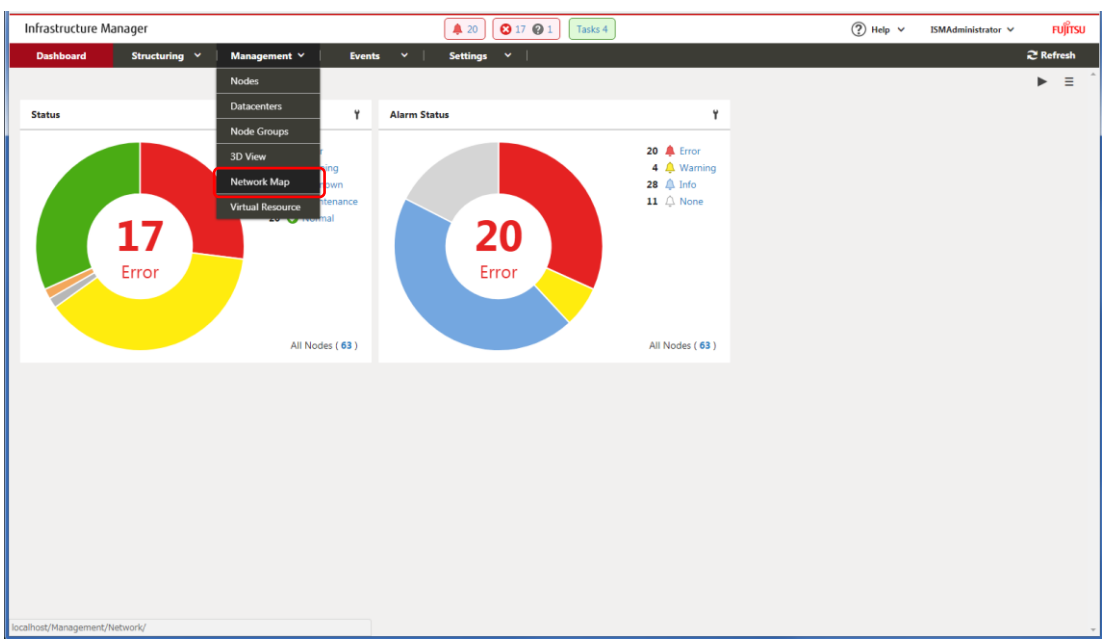
For details, refer to the "2.1.2 FTP Access" in "User's Manual."

Note

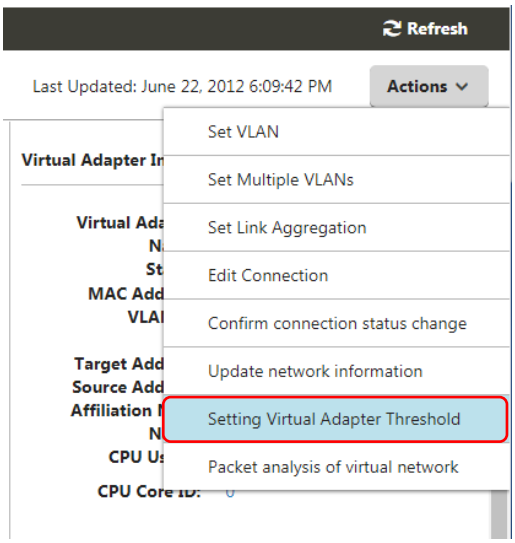
- VM image to be used varies according to the type of hypervisor (VMware, KVM).

2.3. Threshold Value Settings

I. Log in to ISM GUI and select [Management] - [Network Map].

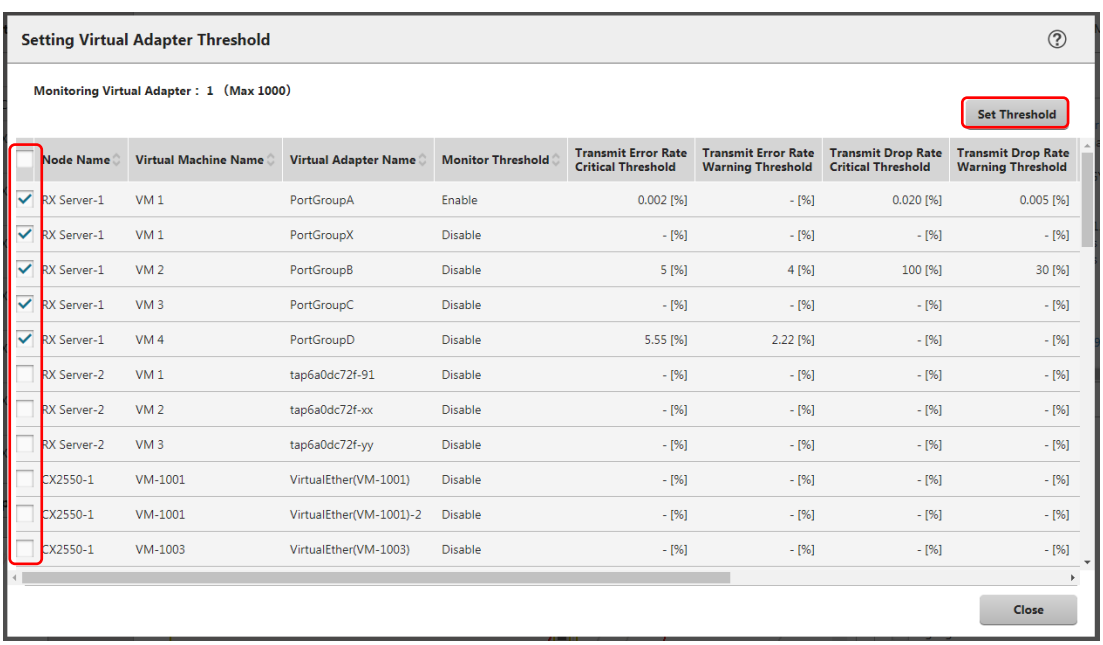


II. Select [Actions] - [Setting Virtual Adapter Threshold].



III. Check the virtual adapter names and select the ports to be monitored.

IV. Select [Set Threshold] button.

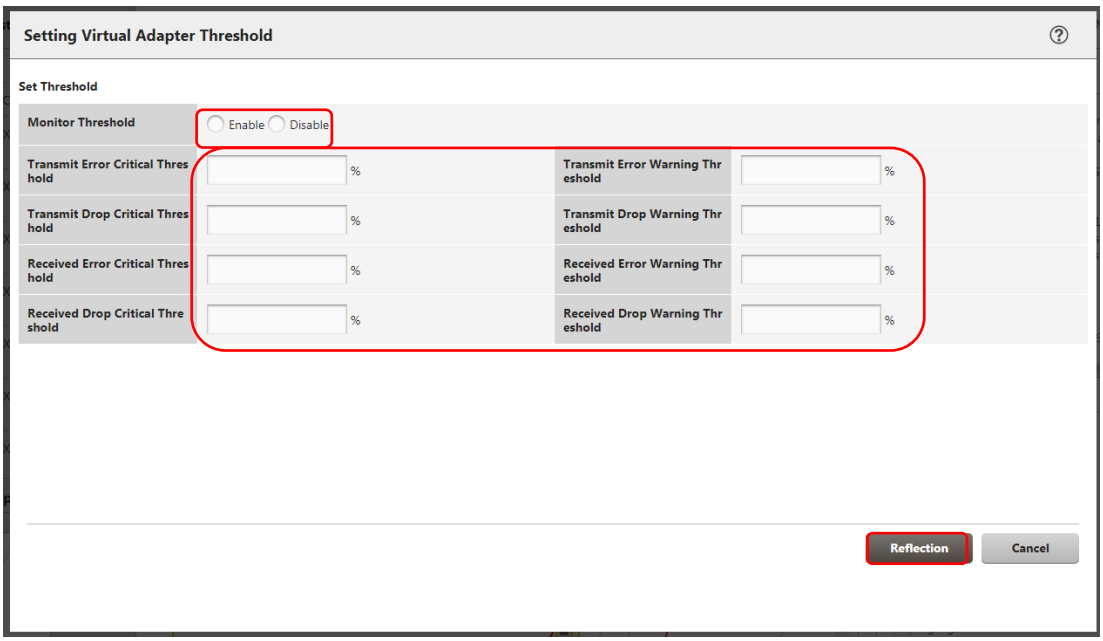


Node Name	Virtual Machine Name	Virtual Adapter Name	Monitor Threshold	Transmit Error Rate Critical Threshold	Transmit Error Rate Warning Threshold	Transmit Drop Rate Critical Threshold	Transmit Drop Rate Warning Threshold
RX Server-1	VM 1	PortGroupA	Enable	0.002 [%]	- [%]	0.020 [%]	0.005 [%]
RX Server-1	VM 1	PortGroupX	Disable	- [%]	- [%]	- [%]	- [%]
RX Server-1	VM 2	PortGroupB	Disable	5 [%]	4 [%]	100 [%]	30 [%]
RX Server-1	VM 3	PortGroupC	Disable	- [%]	- [%]	- [%]	- [%]
RX Server-1	VM 4	PortGroupD	Disable	5.55 [%]	2.22 [%]	- [%]	- [%]
RX Server-2	VM 1	tap6a0dc72f-91	Disable	- [%]	- [%]	- [%]	- [%]
RX Server-2	VM 2	tap6a0dc72f-xx	Disable	- [%]	- [%]	- [%]	- [%]
RX Server-2	VM 3	tap6a0dc72f-yy	Disable	- [%]	- [%]	- [%]	- [%]
CX2550-1	VM-1001	VirtualEther(VM-1001)	Disable	- [%]	- [%]	- [%]	- [%]
CX2550-1	VM-1001	VirtualEther(VM-1001)-2	Disable	- [%]	- [%]	- [%]	- [%]
CX2550-1	VM-1003	VirtualEther(VM-1003)	Disable	- [%]	- [%]	- [%]	- [%]

Point

- If actions for the threshold value setting is selected with a node, virtual machine or virtual adapter selected on the Network Map, the target virtual adapter will be selected.

V. Select [Enable] for Monitor Threshold and after setting the threshold values, select [Reflection].

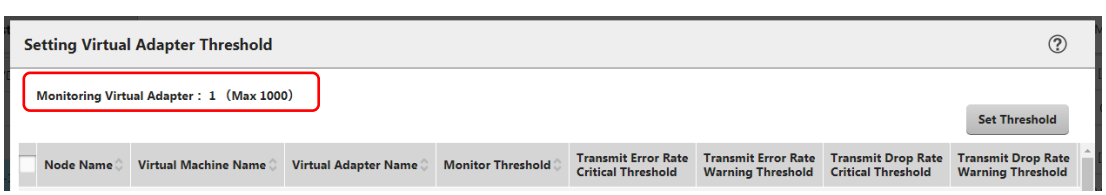


Point

- When you enables Monitor Threshold, monitoring the virtual adapters is started.
- When you disables Monitor Threshold, monitoring the virtual adapters is stopped.
- When you enter threshold values, monitoring the threshold values is started.
- When you delete threshold values, monitoring the threshold values is stopped.
  *Obtaining information will continue.

2.3.1. Precautions for Setting Threshold Values of Virtual Adapter

- The number of the virtual adapter that can be monitored is maximum 1000.
  You can check the number of ports being monitored currently from "Monitoring Virtual Adapter" displayed on the upper side of the setting threshold screen.



2.4. Notification Check

If any event that exceeds the threshold values of the virtual adapter is occurred, the following message will be displayed on [Events] - [Operation Log].

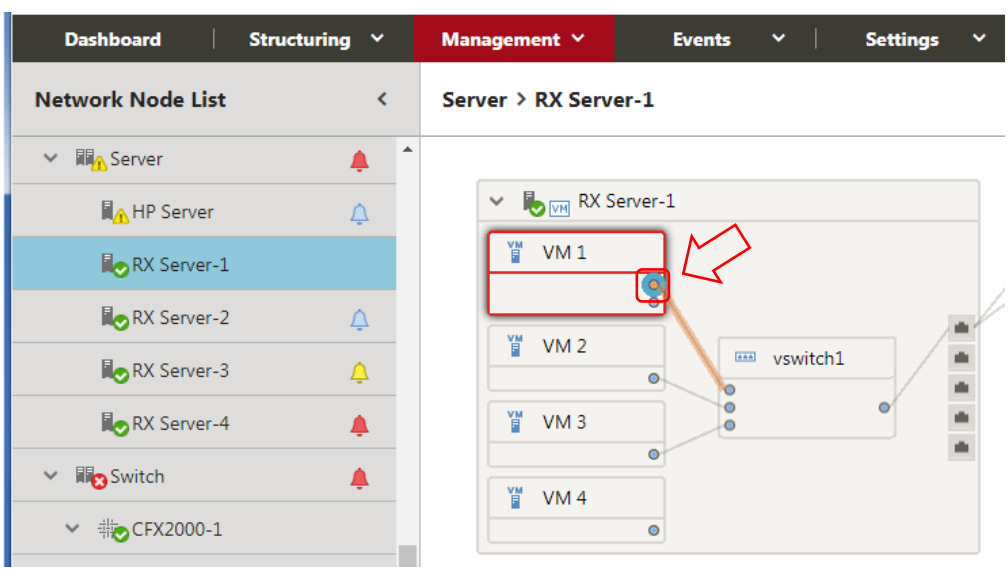
Event ID	Message
30030112	The upper warning threshold value was exceeded at the virtual adapter 'virtual adapter name' of the virtual machine 'virtual machine name'. The monitoring item 'monitoring item name' with value 'measured value' exceeded threshold 'value set by user'.
50030114	The upper abnormal limit threshold value was exceeded at the virtual adapter 'virtual adapter name' of the virtual machine 'virtual machine name'. The monitoring item 'monitoring item name' with value 'measured value' exceeded threshold 'value set by user'.

2.5. Traffic Check

I. Select an applicable [Virtual Network Adapter].

II. Select the node that was detected in the event in the above section 2.4.

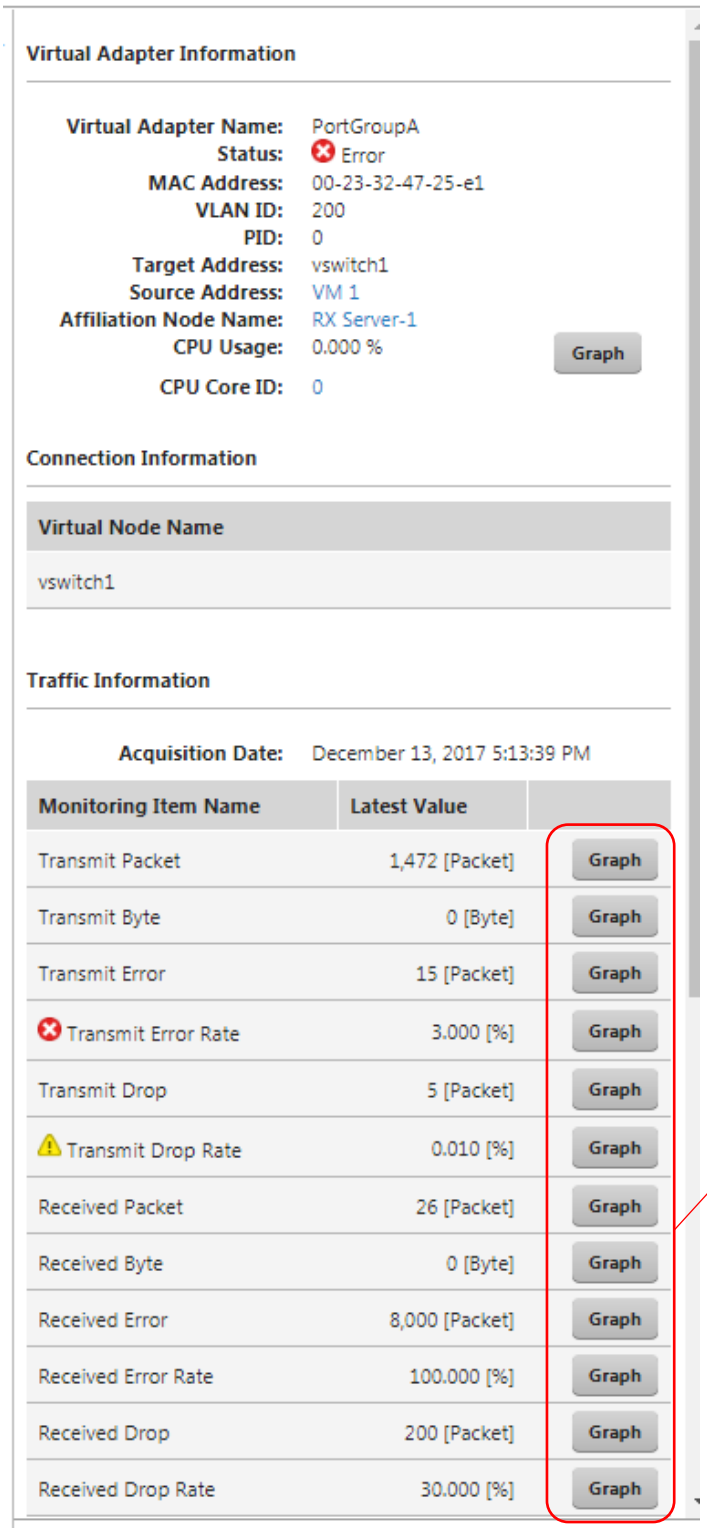
III. Select the virtual adapter name shown in the message of event detected in the section 2.4. Otherwise, select the virtual adapter name highlighted in the virtual machine that was notified in the event.



IV. Scroll the bar downward on the [Virtual Adapter Information] window displayed in the right pane to see [Traffic Information].

Meanwhile, by selecting the [Graph] button located on the right of the information, you can check the transition of the monitored data on a graph.

In ISM 2.3.0.b or later, changes in every monitoring data can be checked simultaneously from the [Graph] button on the right side of [Traffic Information].



Virtual Adapter Information

Virtual Adapter Name:	PortGroupA
Status:	Error
MAC Address:	00-23-32-47-25-e1
VLAN ID:	200
PID:	0
Target Address:	vswitch1
Source Address:	VM 1
Affiliation Node Name:	RX Server-1
CPU Usage:	0.000 %
CPU Core ID:	0

Graph

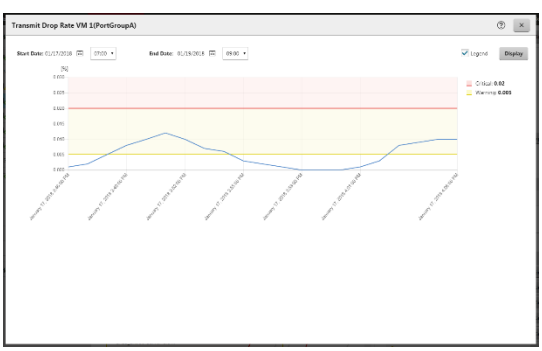
Connection Information

Virtual Node Name
vswitch1

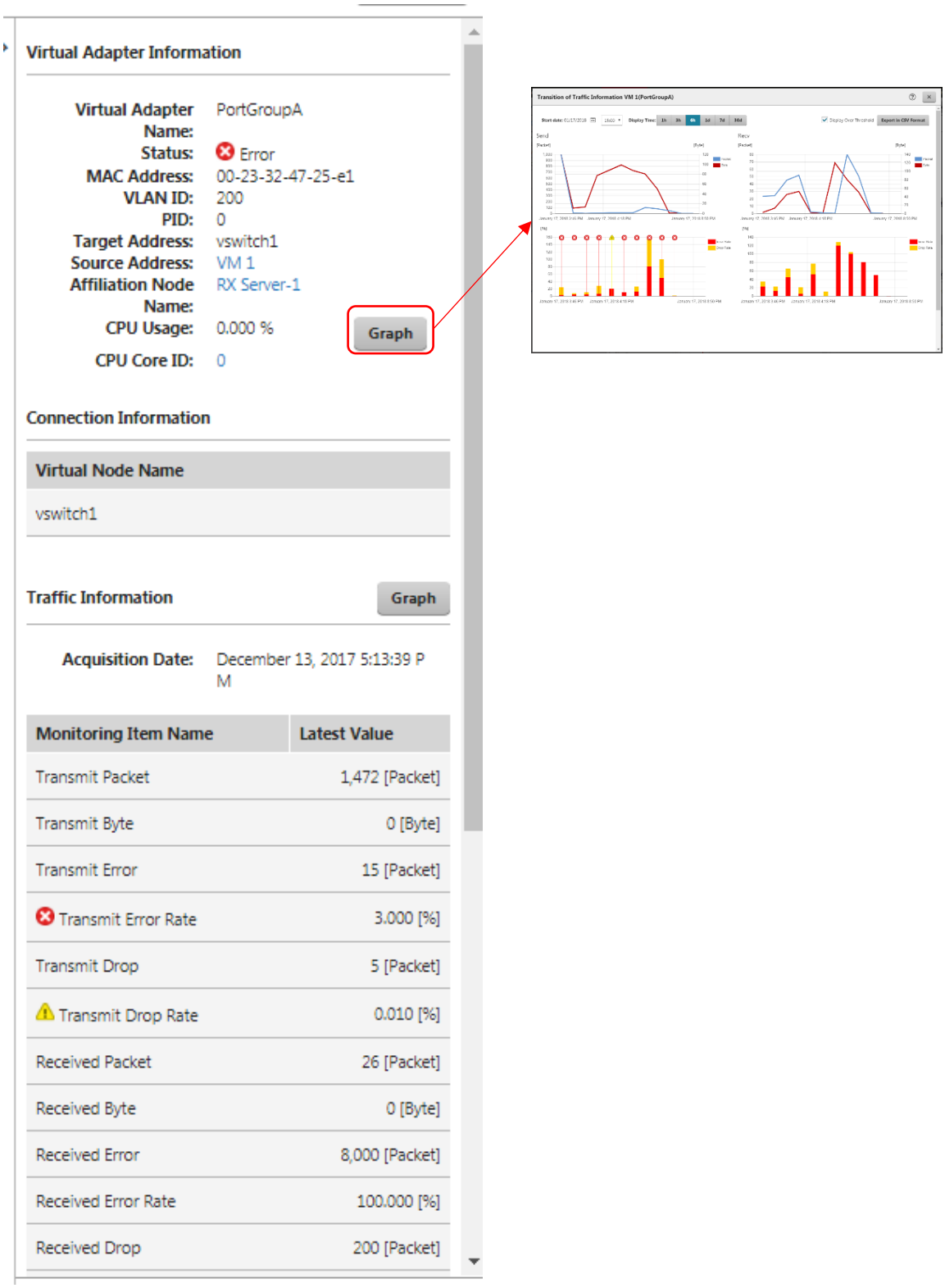
Traffic Information

Acquisition Date: December 13, 2017 5:13:39 PM

Monitoring Item Name	Latest Value	
Transmit Packet	1,472 [Packet]	Graph
Transmit Byte	0 [Byte]	Graph
Transmit Error	15 [Packet]	Graph
Transmit Error Rate	3.000 [%]	Graph
Transmit Drop	5 [Packet]	Graph
Transmit Drop Rate	0.010 [%]	Graph
Received Packet	26 [Packet]	Graph
Received Byte	0 [Byte]	Graph
Received Error	8,000 [Packet]	Graph
Received Error Rate	100.000 [%]	Graph
Received Drop	200 [Packet]	Graph
Received Drop Rate	30.000 [%]	Graph



Example of the [Virtual Adapter Information] and graph display in ISM 2.3.0 / 2.3.0.a



Example of the [Virtual Adapter Information] and graph display in ISM 2.3.0.b or later.

2.6. Packet Analysis

2.6.1. Start of Packet Analysis

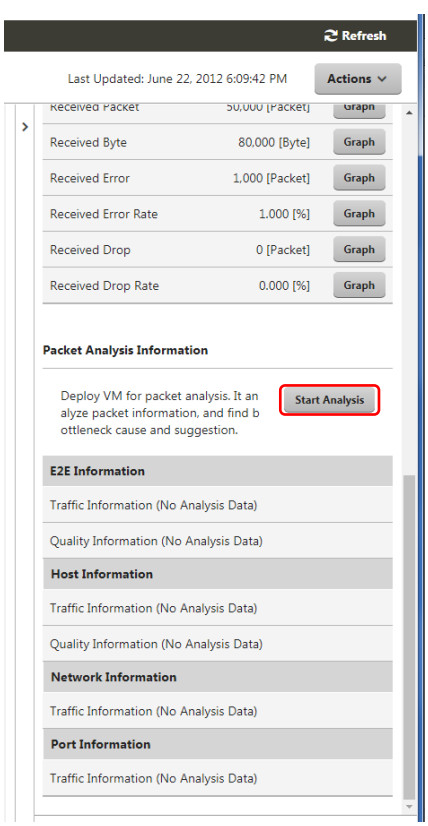
If the cause of performance degradation cannot be identified even by completing up to the section 2.5, execute the packet analysis of the host where the event is being occurred.

Before executing the packet analysis, there are some precautions.
Refer to the "Section 2.6.2 Precautions before Execution of Packet Analysis."

Note

- If the condition has been improved after addressing the cause as a result of checking the packet analysis outcome, stop the packet analysis.
- Once the packet analysis is started, do not delete or change the node OS account or cloud management software settings.

Deploy Analysis VM for the host OS where the performance failure is being occurred.



Enter the parameters.

Analysis VM IP Address Settings

Item	Description
DHCP / IPv4	IP setting to be set to Analysis VM
IP address	Required if IPv4 is specified.
Subnet mask	Required if IPv4 is specified.
Default gateway	Required if IPv4 is specified. *vCenter will be shown only.
NTP server IP address	It is recommended that you specify NTP server.

Analysis VM Deploy Settings (vCenter)

Item	Description
Analysis VM name	Specify the Analysis VM name.
Analysis VM Image file name	Specify vmdk file of Analysis VM.
Analysis VM ovf file name	Specify ovf file of Analysis VM.
Management port connection * From ISM 2.3.0.b, it is not displayed due to the value is set automatically.	Specify a port group that can be communicated with ISM.
Virtual switch type connected to management port * From ISM 2.3.0.b, it is not displayed due to the value is set automatically.	Select a virtual switch type.
Port group name connected to mirror port * From ISM 2.3.0.b, it is not displayed due to the value is set automatically.	Specify a port group that the virtual adapter belongs to.
Switch name/ovs bridge name * From ISM 2.3.0.b, it is not displayed due to the value is set automatically.	Specify a distributed virtual switch connected to the virtual adapter to be analyzed.
Virtual switch port ID/virtual tap * From ISM 2.3.0.b, it is not displayed due to the value is set automatically.	Specify a port ID of the distributed virtual switch connected to the virtual adapter to be analyzed.
Datastore name	Specify a data store name.
Folder name *Displayed for ISM 2.3.0.b or later.	Specify a folder to deploy the Analysis VM in.
Virtual switch type connected to management port *Displayed for ISM 2.3.0.b or later.	Select the type of virtual switch for the connection destination of the management port.
Virtual switch name	Specify the name of switch that can communicate

*Displayed for ISM 2.3.0.b or later.	with ISM.
Network label / Port group *Displayed for ISM 2.3.0.b or later.	Confirm a connection destination that can communicate with ISM in vCenter and set it. Set the network label if it is a standard switch and the port group name if it is a distributed virtual switch.

Analysis VM Deploy Settings (OpenStack)

Item	Description
Analysis VM name	Specify the Analysis VM name.
Analysis VM Image file name	Specify qcow2 file of Analysis VM.
Network name connected to management port	Specify a network that can be communicated with ISM.
Network name connected to mirror port	Specify a network that the virtual adapter belongs to.
Switch/ovs bridge name	It is automatically entered and the value does not required to be changed.
Distributed virtual switch port ID/virtual tap	Specify a virtual adapter name to be analyzed.
Floating IP address settings	Select if you use floating IP address.
Floating IP address	Floating IP address is specified.
Security group	Specify a security group name to be applied to Analysis VM.
Project name	Specify OpenStack project name that the analysis target belongs to.

2.6.2. Precautions before Execution of Packet Analysis

- Resources require to be obtained in advance because Analysis VM will be deployed on the target host OS.
  For details, refer to the "1.4 System Requirements."
- When Analysis VM is deployed, packet mirror settings will be executed on the target host automatically.
  For details on the settings, refer to the following "[Reference] ISM Settings."
- During the execution of Packet Analysis, the performance of service VM may be degraded due to highly loaded node CPU because the resources on the target host is depleted for analyzing packets.
  Keep in mind this before use.

- For vCenter, the virtual network adapter to be analyzed requires to be connected to the distributed virtual switch.
- For OpenStack, SSH requires to be authenticated in a security group applied to Analysis VM.

[Reference] ISM Settings

VMware: To set up, ReconfigureDvs_Task command is used.

For details on the command, refer to the VMware site.

OpenStack: To set up, OVScommand is used.

```
ovs-vsctl --no-wait --add Bridge [ovsName] mirrors [mirrorUuid] --[setSrcId] get
Port [mirrorTargetName] --[setDstId] get Port [mirrorDestName] --[setId] create
Mirror [setmirrorName] [setSelectPort] [setOutputPort]
```

[Reference：When measured in Fujitsu environment]

There is a possibility that the performance of the service VM will be downgraded by approximately 10%.

2.6.3. Analysis Status Check

Select [Events] - [Events] and check events in [Operation Log].

Event ID	Message	Action
10030037	Setting of virtual network analysis was completed (Analysis VM: analysis virtual machine name). *For ISM 2.3.0 and ISM 2.3.0.a. Packet Analysis setting was completed (Analysis VM: analysis virtual machine name). *For ISM 2.3.0.b or later.	Check the result of Packet Analysis per the "2.7 Packet Analysis Result Check."
50035216	An error has occurred while deploying of virtual network analysis. Deployment of analysis virtual machine (analysis virtual machine name) failed. *For ISM 2.3.0 and ISM 2.3.0.a. An error has occurred while deploying of packet	Specify the correct input parameter and execute again. Or check the status of Cloud Management Software. For the following error message, check the ISM version in "2.2.1

	analysis. Analysis virtual machine (analysis virtual machine name) deploying was failed. (Error: error message) *For ISM 2.3.0.b or later.	Obtaining Analysis VM" and the support table of the Analysis VM version, specify the correct Analysis VM file name and then execute again. *For ISM 2.3.0.b or later, it is displayed. “The file 'file name' is not correct” “The version 'analysis VM version' is not support”.
50035217	An error has occurred while deploying of virtual network analysis. Setting of analysis virtual machine (analysis virtual machine name) failed. *For ISM 2.3.0 and ISM 2.3.0.a. An error has occurred while deploying of packet analysis. Analysis virtual machine (analysis virtual machine name) setting was failed. (Error: error message) *For ISM 2.3.0.b or later. * Refer to the message list for Event ID50035217 Error.	Specify the correct input parameter and execute again. Or check the status of Cloud Management Software. *For ISM 2.3.0.b or later, the error messages in the following separate list are displayed. Respond to the error messages.
50035220	An error has occurred while deploying of virtual network analysis. A set file is illegal (Analysis VM: analysis virtual machine name).	Specify the correct file name and execute again. *This message is displayed only for ISM 2.3.0 and 2.3.0.a.

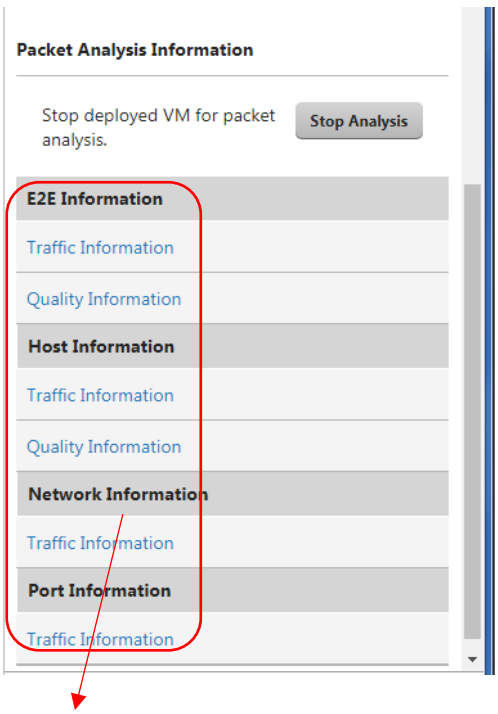
Event ID50035217 Error Message List

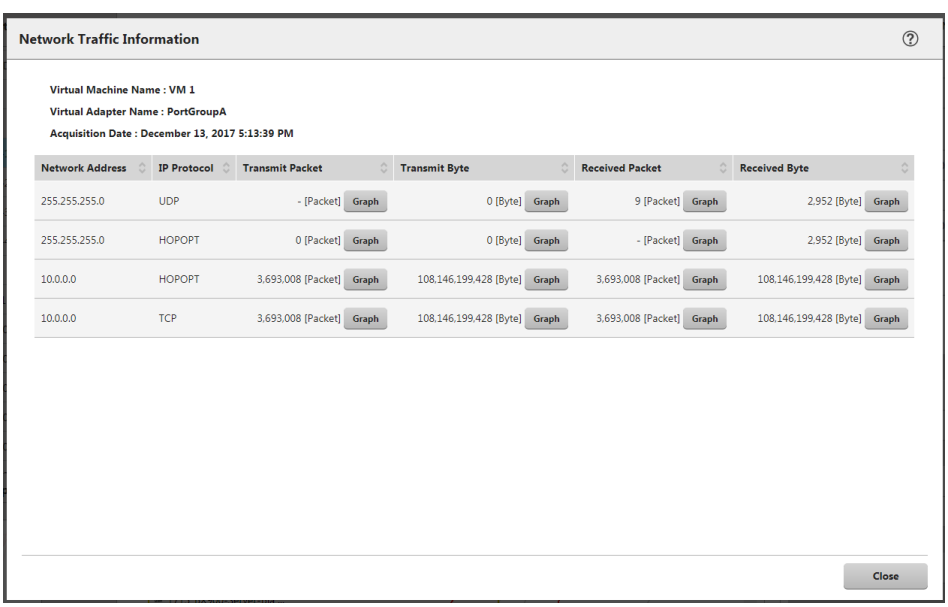
Message	Action
"vCenter: xxxx"	Displays the message sent from vCenter. Check vCenter.
"OpenStack: xxxx"	Displays the message sent from OpenStack. Check OpenStack.
The file 'xxxx' is not correct.	Check the file name of the specified Analysis VM.
The version 'x.x.x' is not supported.	Check the version of Analysis VM.
The VM name 'xxxx' already exists.	Change the name of Analysis VM.

Unable to find the datastore 'xxxx'.	Check the datastore name.
Unable to find the VM folder 'xxxx'.	Check the VM folder name.
Unable to find the switch 'xxxx'.	Check the virtual switch name.
Unable to find the port group 'xxxx'.	Check the network label/port group name.
Unable to find security_group with name or id 'xxxx'.	Check the security group name or the security group ID.
The network 'xxxx' does not exist.	Check the network name.
Cannot complete login to vCnter due to an incorrect user name or password.	Check the user name and password for the vCenter in the Cloud Management Software settings.
Cannot complete login to ESXi due to an incorrect user name or password.	Check the OS tab in the Details of Node screen and check the user name and password of ESXi.
Cannot complete login due to an incorrect IP address.	Check the IP address of Analysis VM.
The request you have made requires authentication.	Check the authentication settings of OpenStack.
There may be insufficient memory	Check the resources of the server of the deployment location for Analysis VM.

2.7. Packet Analysis Result Check

After approximately 10 minutes passed, select each item to see the information.



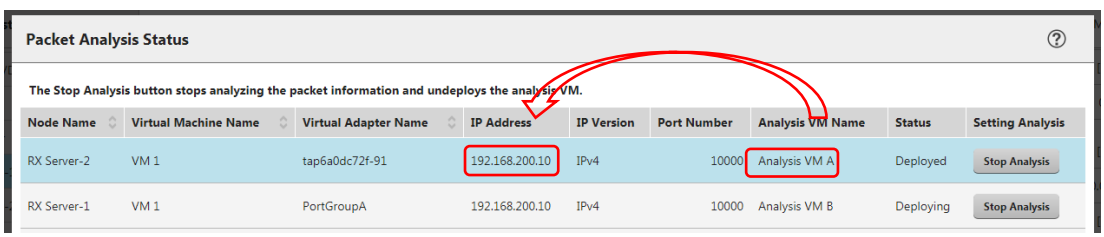


2.7.1. Precautions on the Display Results for Packet Analysis

・ If a result data is not displayed even when Packet Analysis is started for the host registered in vCenter, check if the IP address of Analysis VM shown on ISM matches the IP address of Analysis VM shown in Cloud Management Software.

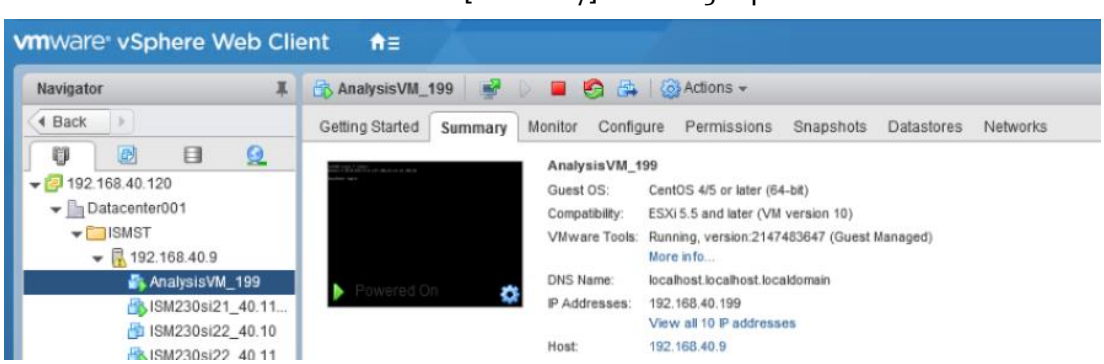
How to check the IP address of Analysis VM on ISM

I. Log in to ISM.
II. Select [Management] - [Network Map].
III. Select [Actions] – [Packet Analysis Status].
IV. Check the [IP address] shown for the applicable [Analysis VM Name].



How to check the IP address of Analysis VM in vCenter / vCSA

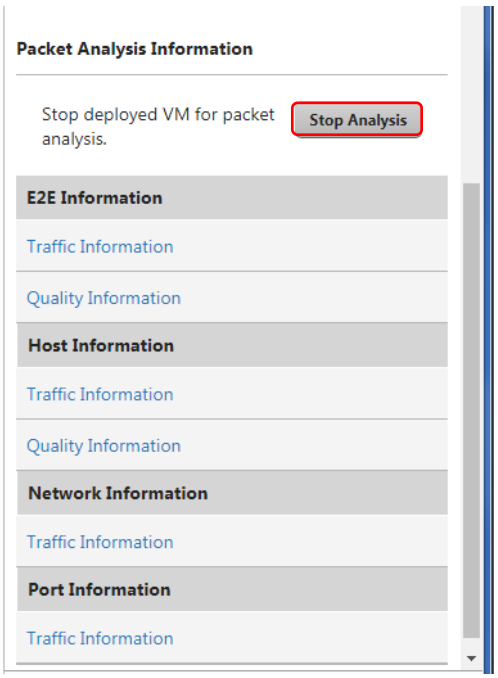
I. Log in to vCenter / vCSA.
II. Select the server to be analyzed from the [Hosts and Clusters] list.
III. Select [Analysis VM Name].
IV. Check the IP address shown in the [Summary] in the right pane on the screen.



・ The results of the packet analysis will not be displayed if Analysis VM itself is migrated. In that case, execute the "2.8 End of Packet Analysis" and restart the packet analysis.

2.8. End of Packet Analysis

Select the [Stop Analysis] button.



Analysis VM will be deleted from Cloud Management Software.

2.9. Differences between VMware and KVM in terms of Packet Analysis of Virtual Network

Functions supported	Display Item	VMware	KVM
I. Statistical performance information obtained from the monitoring target host.	CPU usage	Y *1	Y
	CPU usage of VM vCPU	Y	Y
	CPU usage of virtual network adapter	Y *2	Y
	Traffic information of virtual network adapter	Y *3	Y
II. Information on volume and quality of the traffic from the packet analysis	Port traffic information	Y	Y
	Network traffic information	Y	Y
	Host traffic information	Y	Y
	Host quality information	Y	Y

*1 Information on process CPU utilization cannot be displayed.

*2 Information on CPU scheduler cannot be displayed.

*3 The number of dropped packets only can be displayed.

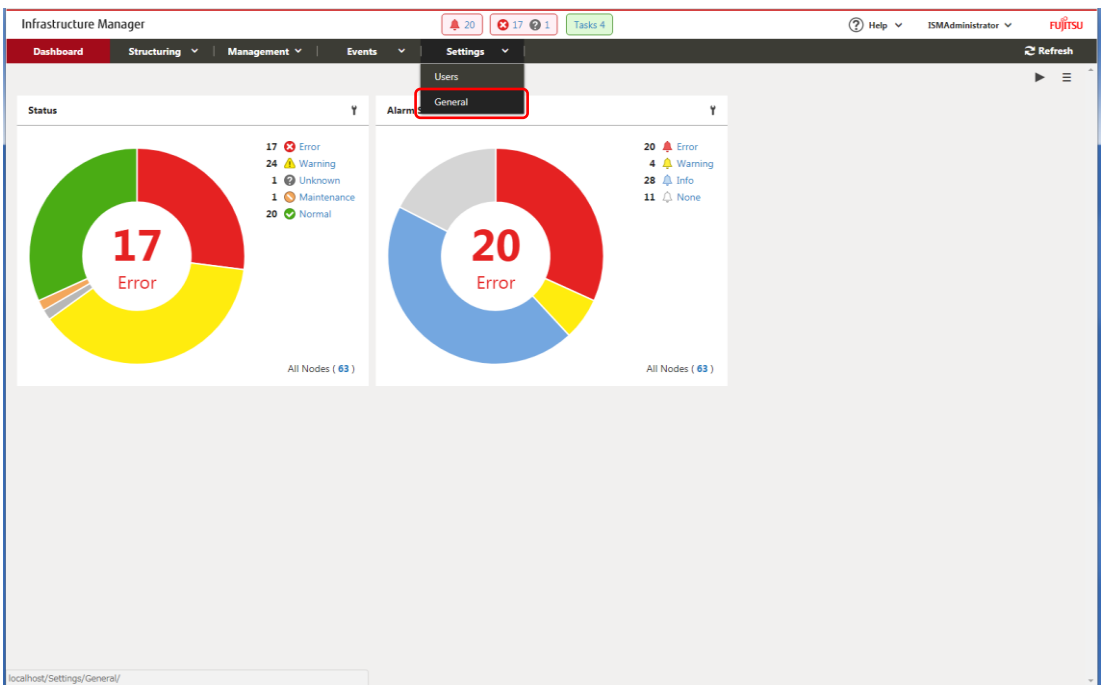
Note

・Xen cannot be used.

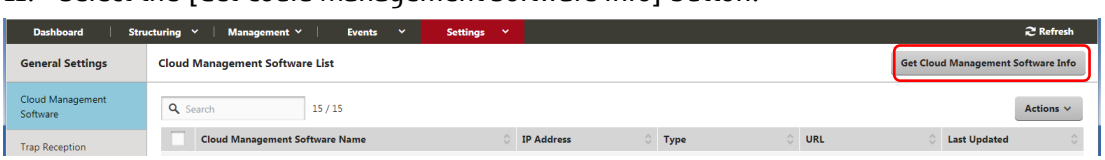
2.10. Precautions When Migration Occurs

When VM migration is executed, re-obtain the information according to the following procedures.

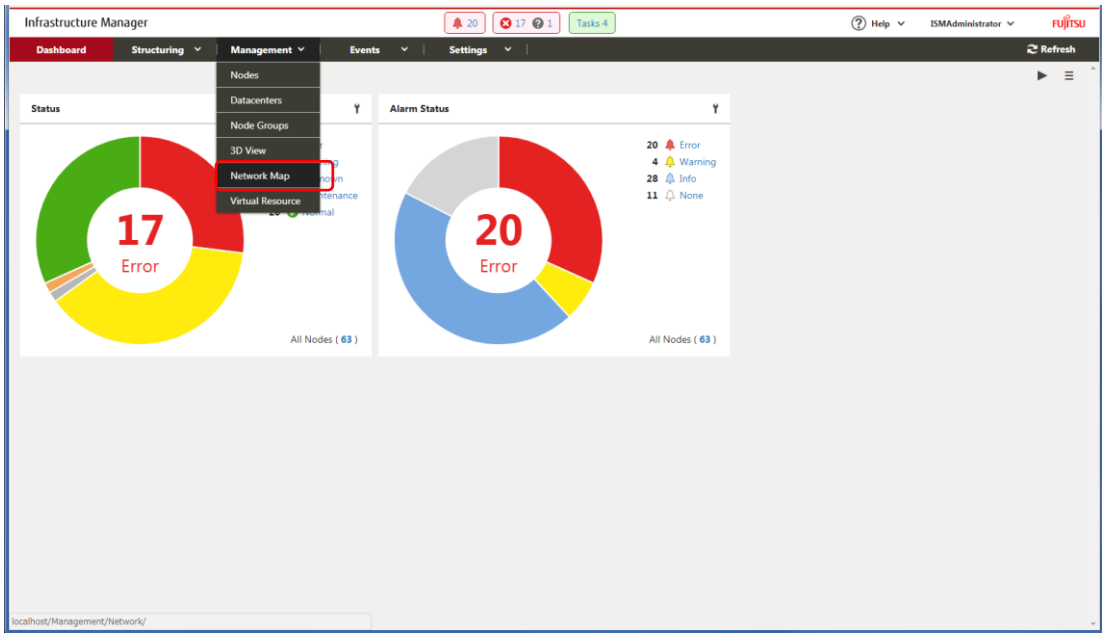
I. Select [Settings] – [General] – [Could Management Software].



II. Select the [Get Could Management Software Info] button.



III. Select [Management] - [Network Map].



IV. Select [Actions] - [Update network information].