Getting Started Guide

Operations Center 5.5

November 18, 2014

Legal Notices

Contents

About This Guide

The *Getting Started Guide* provides both an overview of all the functionality and components of the Operations Center solution as well as guidance on installing it in your environment.

Audience

This guide is intended for the Operations Center administrator who will install and administer the product.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the *User Comments* feature at the bottom of each page of the online documentation.

Additional Documentation & Documentation Updates

This guide is part of the Operations Center documentation set. For the most recent version of the *Getting Started Guide* and a complete list of publications supporting Operations Center, visit our Online Documentation Web Site at Operations Center 5.5 online documentation.

The Operations Center documentation set is also available as PDF files on the installation CD or ISO; and is delivered as part of the online help accessible from multiple locations in Operations Center depending on the product component.

Next, you may wish to refer to:

- *Operations Center 5.5 Release Notes*
- *Operations Center 5.5 Server Installation Guide*
- *Operations Center 5.5 User Guide*
- *Operations Center 5.5 Server Configuration Guide*

Additional Resources

We encourage you to use the following additional resources on the Web:

- NetIQ User Community: A Web-based community with a variety of discussion topics.

- NetIQ Support Knowledgebase: A collection of in-depth technical articles.
- NetIQ Support Forums: A Web location where product users can discuss NetIQ product functionality and advice with other product users.

Technical Support

You can learn more about the policies and procedures of NetIQ Technical Support by accessing its Technical Support Guide.

Use these resources for support specific to Operations Center:

- Telephone in Canada and the United States: 1-800-858-4000
- Telephone outside the United States: 1-801-861-4000
- E-mail: support@netiq.com
- Submit a Service Request

Documentation Conventions

A greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path. The > symbol is also used to connect consecutive links in an element tree structure where you can either click a plus symbol (+) or double-click the elements to expand them.

A trademark symbol (®, ™, etc.) denotes a NetIQ trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a forward slash to preserve case considerations in the UNIX* or Linux* operating systems.

1 Introduction to Operations Center

The *Getting Started Guide* is intended to provide you with all of the overview information that you need in order to use Operations Center. This is the document that you should read first.

This guide provides an overview of all the tools and functionality so that you can determine what best fits your needs. The guide describes all of the components involved with each tool so that you can plan how to integrate Operations Center into your environment. It then provides information and examples for deploying Operations Center, based on your environment. Finally, it explains how to move forward from a test environment to a production environment so that Operations Center is fully integrated into your business.

This guide is organized as follows:

- Chapter 2, "Managing Your Technology and Services with Operations Center," on page 9

  Explains the functionality that Operations Center provides to complete tasks, including the products that provide those functions.
- Chapter 3, "Operations Center Tools & Components," on page 13

  Describes all of the Operations Center tools, and components such as clients, databases, and Web servers.
- Chapter 4, "Supported Versions and Hardware Requirements," on page 27

  Details the supported operating systems, client platforms, databases, and hardware. It includes special requirements for the Dashboard and the Configuration Management System (CMS).
- Chapter 5, "Operations Center Deployment Planning," on page 39

  Provides guidance on how to determine the Operations Center tools to use, then determine how those tools fit within your existing environment.
- Chapter 6, "Environmental Considerations," on page 47

  Explains deployment options for Operations Center, depending upon both the tools and components that you plan to use and your particular environment factors, as follows:
  - Availability and fault tolerance
  - Speed
  - Firewalls
- Chapter 7, "Production Environment Configurations," on page 55

  Provides information on Operations Center configurations and how to replicate it for your production environment.

2 Managing Your Technology and Services with Operations Center

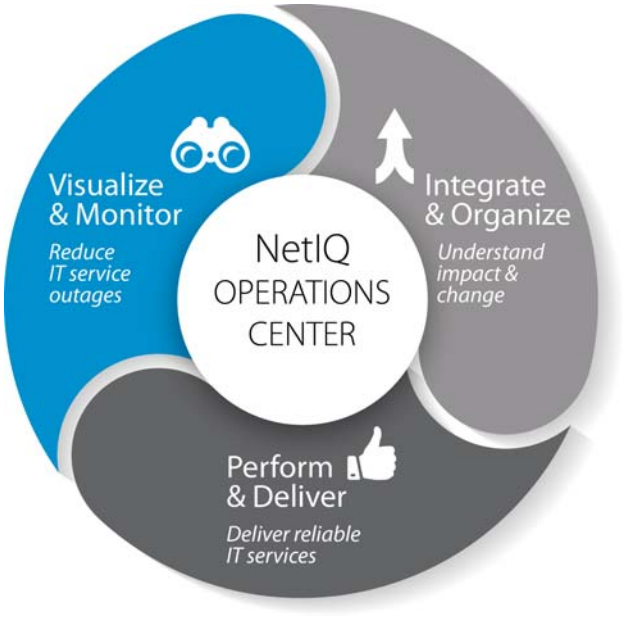
Operations Center provides a platform to integrate information captured by multiple management systems to provide a single view of your technology environment.

Using Operations Center's single, integrated view lets you optimize the:

- **Management of Technology Resources.** Relate data from multiple management systems to understand how one component of an environment impacts other components.
- **Performance of Services Supported by the Technology.**

  Align the integrated data to specific business processes.
- **Responsiveness to Events in the Technology Environment.**

  Translate the integrated data into a consistent set of monitoring and reporting metrics available to managers across the organization.



The Operations Center platform consists of a suite of tools and functionality that offer a wide range of possibilities for design, deployment, and ongoing management of your technology and business environment. While quick and easy to get started, Operations Center offers the ability to be fully customized so that your implementation can be as unique as your business needs, technology environment, and your imagination.

This platform provides a variety of functions that provide the following core competencies:

- Section 2.1, "Integrating Data," on page 10

  Integrate information from all your third-party management systems and other data sources into Operations Center.
- Section 2.2, "Modeling Services," on page 10

  Create services models so that your data accurately represents its impact on your business and you can use these models to monitor and manage service level agreements.
- Section 2.3, "Monitoring," on page 11

  Monitor and manage data through element status and alarms.

- Section 2.4, “Visualizing Data,” on page 11

  Create visualizations of data to quickly provide an accurate view of the status of IT services.
- Section 2.5, “Managing Services,” on page 12

  Use service models to monitor and manage services using service level agreements.

2.1 Integrating Data

Operations Center is designed to connect to multiple systems and data sources to capture events, alarms, elements, models, and relationships; and then apply logic to that data to create a hierarchy of managed objects (or elements). In this way, you get a visual representation of your resources, and the management systems that monitor and report on their operating status and performance, that reveals both status and relationships.

Using Operations Center tools, you can:

- Integrate with popular third-party IT management systems, trouble ticket software, and discovery tools. With Operations Center’s directional access to many of the underlying management systems, you can perform actions against monitored systems, such as acknowledging or closing an alarm. and control IT resources as a seamless component of the IT and business environment.

  For a list of supported management systems, see Chapter 4, “Supported Versions and Hardware Requirements,” on page 27. For instructions on integrating, see the *Operations Center 5.5 Adapter and Integration Guide*.
- Leverage business metrics, help desk tickets, and other information stored in your databases. For information, see *Operations Center 5.5 Data Integrator Guide*
- Gather end user, synthetic testing, and application performance data from Web sites and Web applications. For information, see *Operations Center 5.5 Experience Manager Guide*
- Capture line-oriented event data from nearly any source. Perfect for leveraging data from sources like niche or homegrown tools, as well as Remedy Help Desk. For information, see *Operations Center 5.5 Event Manager Guide*
- Integrate data using SNMP polling. For information, see *Operations Center 5.5 SNMP Integrator Guide*
- Use the API to interact with some elements, and query performance metrics, from remote third-party applications. For more information, see the *Operations Center 5.5 Web Services Guide*.

2.2 Modeling Services

Service Models are used to logically group physical IT infrastructure elements into the context of business services and processes to:

- depict the relationship between IT resources and the services they support across management systems, businesses process, and even companies
- provide an end-to-end view of the current state of the elements across an enterprise
- provide a business view of an environment

Each service model presents a set of elements in a hierarchy that represents the relationships among the elements. It includes dynamic relationships that allow for monitoring of elements in real-time and the collection of data to determine the performance of elements as they impact the overall service.

The dynamic building and maintaining of service models, based upon changes in data received from Operations Center integrations with third-party management systems, can be automated to implement modeling on an enterprise level.

For more information about modeling services, see *Operations Center 5.5 Service Modeling Guide*.

2.3 Monitoring

Effectively monitor and manage availability and performance of applications and IT services that you deliver to business.

Through the hierarchy and service models, data is organized as elements and relationships are established among elements in terms of their impact on your business and its services. Operations Center monitors the impact of poor performance of one element on other elements in terms of your ability to provide business services. You are alerted to not only outages, but any risk of outages.

Active monitoring includes the use of:

- **Element State Propagation.** By default, an element's state is calculated by inheriting the condition of it's most critical child. Alternate algorithms can be used to apply a sequence of calculations to control state propagations and update with conditions that more accurately reflect the overall status of the business or technology it represents. See *Using Algorithms to Calculate Element State* in the *Operations Center 5.5 Server Configuration Guide*.
- **Alarms.** Alarms are used as mechanisms to indicate when an event occurs and are associated with specific events. Each alarm has a severity level. In addition to simply monitoring alarms, actions can be taken on some alarms, depending on the management system from which the element originated. See *Filtering and Managing Alarms* in the *Operations Center 5.5 User Guide*.
- **Automation Events & Alerts.** An automation event is an action triggered by an activity or condition change that occurs in a network. Automation events are defined to notify the appropriate personnel that an event occurred and might require intervention. Automation alerts can include audio signals, notifications sent via e-mail, or entering information in a database about an event. Automation events can be either client side or server side. See *Defining and Managing Automation Events* in the *Operations Center 5.5 Server Configuration Guide*.
- **Custom Complex Actions.** Use scripting capabilities to define more complex actions, such as tracking actions performed on alarms.

For monitoring overview, see the *Operations Center 5.5 User Guide*. For information on configuring options for alarms, algorithms, and automations, see the *Operations Center 5.5 Server Configuration Guide*.

2.4 Visualizing Data

Operations Manager has various views to help you visualize your data and its impact on your business services. Operations Center console provides various console views and portlets of data that includes visualization, hierarchies, charts, relationships and impact summaries:

- **Navigational Network Diagram.** A dynamic graphical interface that enables moving across the entire enterprise, managing applications, servers, and network components. The network view displays relationships among system components within a large infrastructure with the selected element at the center, with spokes connecting to child elements. The line colors identify the conditions of the child elements. The Network View is a feature of the Operations Center console.

- **Relationships.** Enhanced visualization and navigation of element relationships. The Relationship view is a feature of the Operations Center console and dashboard.
- **Performance Charts & Reporting.** Chart real-time and historical data from some management systems. The performance view is available in the console as well as in the dashboard. Performance data is also analyzed for service level agreements with the Performance Analysis window, a features of the Service Level Management tool. In addition, reports on data are available via Dashboard portlets. You can also create custom reports using third-party tools by using SQL Views. For more information on SQL Views, see *Operations Center 5.5 SQL Views Guide*.
- **Layout Diagrams and Drawings.** A visual analysis of critical relationships and conditions across multiple element hierarchies. The dynamic linking feature binds graphics in a drawing to element conditions and attributes, thus enabling automatic updates of the drawing when elements change. A set of drawing tools for adding shapes, colors, text, and many other features found in standard drawing products gives you full control of your representation. Build Layout drawings in the Operations Center console which are then published to others in the Dashboard. For more information about the layout drawings, see the *Operations Center 5.5 Custom Drawing and Layout Guide*.

For information about console views, see the *Operations Center 5.5 User Guide*. For more information about Dashboard portlets, see the *Operations Center 5.5 Dashboard Guide*.

2.5 Managing Services

To help manage services, you can configure, manage, and monitor Service level agreements (SLAs). An SLA is a contract between a service provider and a customer that specifies in measurable terms the service to be provided.

Operations Center tools, particularly the Service Level Manager, allow you to define service level agreements, and monitor and manage those agreements. Reports on SLA data are available in the dashboard.

For information on configuring SLAs, see the *Operations Center 5.5 Service Level Agreement Guide*. For information about the Dashboard, see the *Operations Center 5.5 Dashboard Guide*.

3 Operations Center Tools & Components

Operations Center tools and components must not only work together, but also interact with existing components in your environment. As you read through the description of the components, determine the components that you want to install based on the products that you intend to use for your Operations Center solution and the third-party systems that are needed to support those components.

When installing Operations Center tools and components, there are minimum hardware requirements that must be met and certain version of third-party systems that are supported. Keep in mind that requirements vary, depending on the site, and might be higher because of the size of your organization's managed infrastructure.

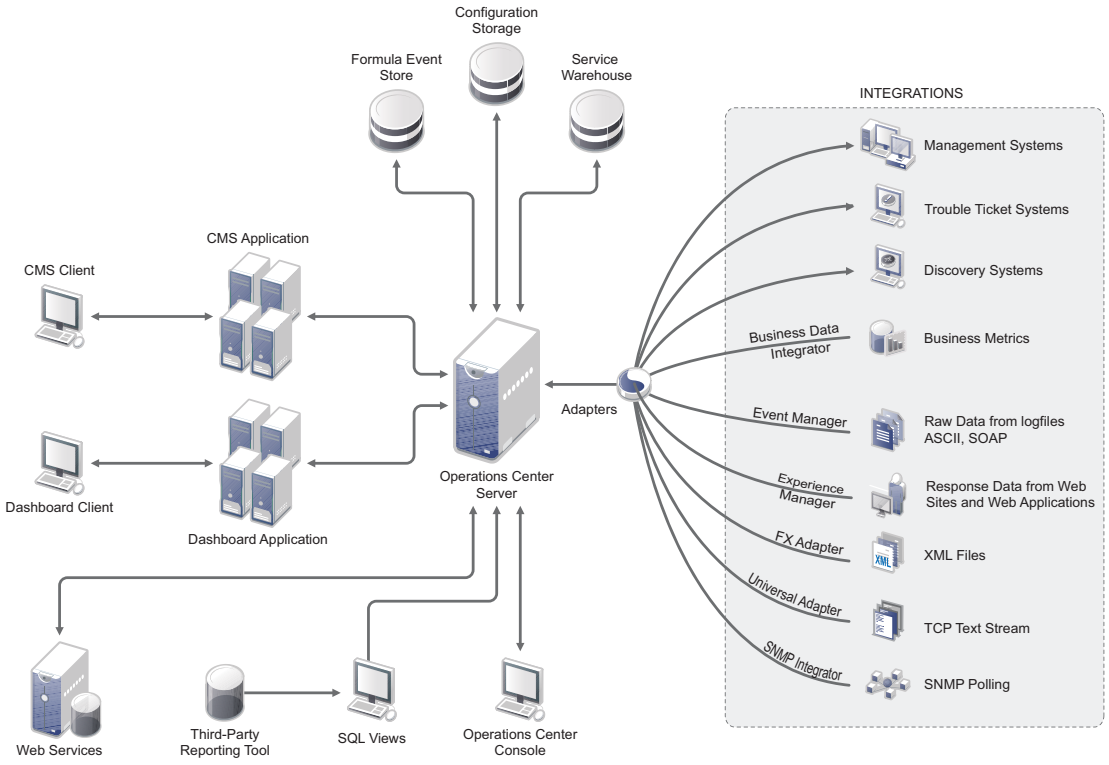
For more information about installation and configuration, see the *Operations Center 5.5 Server Installation Guide* and the *Operations Center 5.5 Server Configuration Guide*, respectively. For information on operating systems, databases, and third-party systems for which support is being discontinued, see the *Operations Center 5.5 Release Notes*.

Review the following sections to understand these components and tools:

3.1 Operations Center Architecture

Figure 3-1 is a simple illustration of the architecture of the Operations Center solution. Different deployment scenarios are explained in the later sections of this guide.

Figure 3-1 *General Operations Center Solutions Architecture*



The Operations Center server is the main component of the Operations Center solution. Management systems, including both third-party tools and other Operations Center tools, integrate data into Operations Center, and users can perform operations on the management systems from the Operations Center console.

The Operations Center server interacts with three data stores. Other products have embedded databases.

The Dashboard is a Web application, which also functions as a client to the Operations Center server. It allows users to view and manipulate data from the Operations Center server. Even though the dashboard can optionally be installed on the same host machine as the Operations Center server, it is advisable to install on different machines.

Web Services allows third-party applications access to data in the Operations Center server. SQL Views allows read access to data to create reports using a third-party reporting tool.

3.2 Operations Center Tools

A suite of tools supports all of the functionality that Operations Center solution offers. The main components of Operations Center are the Operations Center server and console with various other tools that work in conjunction with the server.

Table 3-1 shows the products that are needed to complete the listed functions:

Table 3-1 *Functions and Products*

Function	Tools
Security management	Console, Dashboard
Management system data integration	Console, Adapters, Experience Manager, Event Manager, F/X Adapter, Guard, SNMP Integrator
Discovery data integration	Console, Adapters
Trouble ticket data integration	Console, Adapters, Business Data Integrator
Service modeling	Console, Service Configuration Manager
Monitoring (alarms, automation)	Console, Dashboard, NOC Script
Visualization	Console, Dashboard
Service level agreements	Console, Dashboard, Service Level Manager
Configuration management database	Console, CMS
Reporting	Dashboard, SQL Views
Version tracking	Console, SQL Views
Customizing	NOC Script

The following Operations Center tools are available:

3.2.1 Adapters

An adapter is the integration point that allows the Operations Center server to connect to a management system. The adapter not only provides information from the third-party management system to the Operations Center server but also replicates much of the functionality available in the management system.

Adapters provide bidirectional access to many of the underlying management systems in order to allow end users to perform actions against monitored systems such as acknowledging or closing an alarm. This allows IT managers to control IT resources as a seamless component of the IT and business environment.

Different Operations Center adapters exist for each different third-party management system, and adapters are configured with a one-to-one relationship. That is, each adapter connects a Operations Center server to one specific instance of a third-party management system. Each adapter is written to the specific API that integrates bidirectionally with that system.

An Object Request Broker (ORB) is required for some adapters to broker the communication between the Operations Center adapter and the third-party management system with which it communicates.ORBs, which are written in C++ or Java, resides on the management system that is connected to the Operations Center adapter.

For more information about integration adapters, see the *Operations Center 5.5 Adapter and Integration Guide*.

3.2.2 Experience Manager

Experience Manager conducts end user, synthetic testing on applications and Web sites and measures performance. Experience Manager emulates end user business processes against applications on a 24x7 basis, including Web and non-Web environments, and applications.

The Experience Manager architecture consists of the following components:

Experience Manager Adapter
Experience Manager Database
Experience Manager Monitors

Experience Manager uses MODL to create a meaningful element hierarchy for the interpretation of metrics.

For more information, see the *Operations Center 5.5 Experience Manager Guide*.

3.2.3 Business Data Integrator (BDI)

Business Data Integrator integrates business metric, help desk tickets, and other information residing in other databases. BDI allows the surfacing of data from any JDBC-compliant database. The Business Data Integrator adapter extracts data from specified sources and integrates it into Operations Center. The BDI Definition Editor is used to create and edit adapter definitions.

For more information, see the *Operations Center 5.5 Data Integrator Guide*.

3.2.4 Event Manager

The Event Manager filters and normalizes line-oriented ASCII (American Standard Code for Information Interchange) event data from sources such as a mainframe environment, telecommunications devices, log files, message traffic, SNMP traps, serial port devices, and telnet sessions. The data is received and identified by a parser and then optionally processed through a rule base. Event messages are constructed from the data and passed to the Operations Center server as an event.

The Event Manager's architecture consists of the following components:

Configuration Manager
Agents and the Agent Manager
Alarm Server
Event Manager

Agents are on a single machine or distributed across multiple machines. It is necessary to define an adapter for each instance of the Event Manager in the network. Only one Event Manager adapter can exist on each machine.

The Event Manager processes alarms in accordance with rulesets. Rulesets provide the Event Manager with instructions on how to process raw event data. Rulesets contain individual rules that provide a set of instructions on parsing and extracting useful information from events. You use the Event Manager Ruleset Editor to create and validate rulesets.

For more information, see the *Operations Center 5.5 Event Manager Guide*.

3.2.5 F/X Adapter

The File and XML (F/X) adapter distributes file and XML-based data collection, parsing, processing, and alarm generation into multiple Operation Center servers. The F/X adapter is a hierarchy-based adapter with the ability to receive alarms from multiple F/X Monitors.

When the adapter receives an alarm, it generates an alarm and processes it through the hierarchy. F/X Monitors dynamically create rich alarms with properties and values derived from a data source, using the parsing rules defined in the Monitor for the data source.

It is necessary to configure F/X Monitors to send alarms to the F/X adapter. You identify the F/X adapter using either an IP address or a hostname and the TCP/IP listen port configured for the adapter.

For more information, see the *Operations Center 5.5 F/X Adapter Guide*.

3.2.6 SNMP Integrator

The SNMP adapter integrates SNMP data gathered from other management technology systems. The SNMP adapter allows you to poll, gather, and view data available on your SNMP agents.

For more information, see the *Operations Center 5.5 SNMP Integrator Guide*.

3.2.7 Service Level Manager

The Service Level Manager is the Operation Center tool for creating, monitoring, and reporting on service level agreements (SLAs). Service Level Manager uses the Service Warehouse to store data related to SLA performance.

For more information, see the *Operations Center 5.5 Service Level Agreement Guide*.

3.2.8 Dashboard

The Operations Center dashboard is a Web-based application that allows users to customize their own Web pages with content from Operation Center as well as other sources. It allows for single sign-on, personalization, and integration of data from different sources.

Portlets, or Web-based applications built for integration into a portal, provide functionality and allow users to view selected content from the Operation Center server as well as other sources. Content, including content alarms from the Operation Center server, can be updated in real time.

For more information, see the *Operations Center 5.5 Dashboard Guide*.

3.2.9 Configuration Management System (CMS)

The Configuration Management System is a Web application that combines Web 2.0 and structured social networking principles to significantly enhance enterprise CMDB usability, accessibility and accuracy—for CMDB projects. It makes CMDB visualization, navigation, search, analysis, and reporting measurably easier and more intuitive, to improve IT service quality.

Because users actively contribute to and maintain the CMS repository information, the risk of changes to the IT infrastructure can be reduced and impacts from outages can be more effectively managed.

For more information, see the *Operations Center 5.5 Configuration Management System (CMS) Guide*.

3.2.10 SQL Views

SQL Views provides functionality in Operation Center that allows for third-party applications to have read access to Operation Center data. The purpose of SQL Views is to take data from the Operation Center server and the Service Warehouse and make it accessible for you to query it and write reports using it.

External products such as Business Objects Crystal Reports or Microsoft Excel can be used to create reports.

In addition to reporting, Operation Center data can also be used by other applications for other business purposes.

3.2.11 Operation Center Scripting Language

Scripts created using NOC Script, formerly called FormulaScript, can be used with various features, including automations and algorithms. Operations Center ships with a library of default scripts, which can be customized to suit your needs. New scripts can also be added to the Script Library.

For more information see the *Operations Center 5.5 Scripting Guide*.

3.2.12 Web Services

Third-party applications can interact with the Operations Center server using the Web Services Application Programmer Interface (WSAPI). This API provides a number of services that allow remote applications to query data that is warehoused in the Operations Center server. You can also use the API to create, update, or remove a limited set of elements.

The Operations Center Web Services tool has two components:

Operations Center Web Services Application Programmer Interface (WSAPI): This is an integration point for third-party applications to interact with the Operations Center server, including querying data and creating, updating, and removing a limited set of data in the Operations Center server.

Operations Center Web Services Client: This is a command-line utility that provides instant access to all available Web services capabilities. It is useful to test various approaches to Web services.

For more information, see the *Operations Center 5.5 Web Services Guide*.

3.3 Mapping Operations Center Tools and Components

Operations Center tools often share similar components. Table 3-2 shows the shared components that are applicable for each product. For more information about the Operations Center tools, see Section 3.2, "Operations Center Tools," on page 15.

Table 3-2 *Tools and Components*

Tools	Operations Center Components
Adapters, including Experience Manager, Business Data Integrator (BDI), Event Manager, F/X Adapter, SNMP Adapter	Operations Center server, Remote Container server, Operations Center console, Configuration Storage, Event Store, Service Warehouse
Service Configuration Manager (SCM)	Operations Center server, Operations Center console, Configuration Storage, Event Store, Service Warehouse
Service Level Manager (SLM)	Operations Center server, Operations Center console, Configuration Storage, Event Store, Service Warehouse
Dashboard	Operations Center server, Web server, Image server, Dashboard client
Configuration Management System (CMS)	Operations Center server, Web server, CMS client
SQL Views	Operations Center server, Operations Center console, Event Data Store
NOC Script	Operations Center server, Event Data Store
Web Services	Operations Center server, Event Data Store

3.4 Operations Center Servers

The Operations Center solution includes the following servers:

- Section 3.4.1, “Operations Center Server,” on page 20

  This is the base server for all Operations Center tools.
- Section 3.4.2, “Remote Container,” on page 20

  Can be used to off-load some resources from the Operations Center server.
- Section 3.4.3, “Web Server,” on page 21

  Allows Web client access to the Operations Center server.
- Section 3.4.4, “Image Server,” on page 22

  Allows Web clients to render dynamic and 3-D charts.

3.4.1 Operations Center Server

The Operations Center server is the main component to the Operations Center solution. It contains the engine that integrates data, manages the hierarchy of data as elements and relationships among them, and performs data calculations.

The Operations Center server has specific requirements for the hardware and software on which it is installed as well as security considerations. For information about ports and database connections, see Section 3.7.1, “Operations Center Server Port Usage,” on page 24.

The Operations Center server accesses other management systems and both Operations Center data sources and external data sources. Users and other Operations Center and third-party products also access the Operations Center server.

For access, you will need the host name and IP address of the machine on which Operations Center server is installed. To install Operations Center server, you will need administrative access to the machine. Operations Center server is configured with a default administrative password which you can change.

3.4.2 Remote Container

The Remote Container server is a scaled down version of the Operations Center server that runs all adapters and integration but has no other functionality (for example, no monitoring, modeling, service level agreement support, and so on).

The Remote Container server has the following uses:

- Distributes the running of adapters and integrations among multiple machines
- Runs adapters or integrations under a different JVM or configuration than the Operations Center server

  The Remote Container can run either 32-bit or 64-bit and can connect to a Operations Center server running 64-bit. If you have a management system that runs on 32-bit, such as BMC Remedy ARS, you could use integrate data from it into a Remote Container server which is also running 32-bit. Then, you could connect your Operations Center server (which is running 64-bit) to the Remote Container server to use the Remedy data in your Operations Center solution.

Similar to other adapters which bring in data from management systems, a Remote Container adapter brings data into the Operations Center server from the Remote Container server:

- Elements appear to be and act as local elements. Operations Center functionality (such as models and SLAs) can be applied to them the same as other elements.
- Creating and administering a Remote Container adapter is different than other adapters in Operations Center. A Remote Container adapter requires a connection be established to a Remote Container server.
- Properties for elements (such as name, time skew, daemon host, daemon port, login account/password) establish the connection. Operations on these elements include creating, starting, stopping, and deleting.

The Remote Container server does not allow client sessions; the only connection is through integration with the Operations Center server. The Remote Container server also does not have an associated Web server.

The Remote Container server is a Java program that runs its own Java Virtual Machine (JVM). It can be installed on the same host machine and use the same daemon as the Operations Center server and uses its own JVM. Or, the Remote Container server can be installed on a different host machine than the Operations Center server.

The hardware and software requirements for the Remote Container host machine are the same as the Operations Center server.

For more information, see *Using Remote Containers* in the *Operations Center 5.5 Adapter and Integration Guide*.

3.4.3 Web Server

A Web Server provides access from Operations Center Web clients to the Operations Center server.

The Operations Center server contains a Web server that is compatible with the Java Servlet and JSP Technologies from Sun Microsystems.The Web server is configured during installation and can be started and stopped. It can also run in either production or development mode. The Web server also has options for auditing.

For more information on configuring the Web server, see *Web Server Pane*, *Configuring Web Server Start and Stop*, and *Using the Web Server* in the *Operations Center 5.5 Server Configuration Guide*.

The dashboard ships with a version of Apache Tomcat, which it uses as its Web server by default. You can opt to use an Apache Web server if it is needed to deploy security or other plug-ins, or if the Web server needs to be customized beyond the options available with the Tomcat server. If users' browsers are required to make HTTP requests through an Apache Web server rather than the dashboard supplied Tomcat server, then you must set up a reverse proxy.

For the current version of Apache Tomcat that the dashboard uses as well as other information about dashboard; see the *Operations Center 5.5 Dashboard Guide*. The Web server for the dashboard can be installed on either the same host machine as the Operations Center server or a different host machine.

3.4.4 Image Server

An Image Server is required by Operations Center to allow Web clients to render dynamic and 3-D charts. The Image Server is installed with the dashboard and requires a Java runtime environment (JRE) and ports for communication. The Image Server must be configured to recognize IP addresses or host names for every URL needed to access Operations Center.

3.5 Clients for Operations Center

The Operations Center solution has multiple clients for accessing the Operations Center server. The functionality available in each client varies. The clients are:

- **Operations Center console.** The main client for accessing most Operations Center functionality and configuration. All functionality for integrations, monitoring, modeling, and service level agreement management is available in the console. For more an overview of the Operations Center console, see the *Operations Center 5.5 User Guide*.
- **Dashboard.** A Web client to the Operations Center server. Build Web pages that include functionality for monitoring alarms, managing service level agreements, and administering users of the Operations Center server.The dashboard allows users to customize their own Web pages with content from Operations Center as well as other sources. It allows for single sign-on, personalization, and integration of data from different sources. For more information, see the *Operations Center 5.5 Dashboard Guide*.
- **Configuration Management System (CMS).** A Web application for CMDB projects, that allow users to actively contribute to and maintain the CMS repository information.For more information, see the *Operations Center 5.5 Configuration Management System (CMS) Guide*.
- **Web Services.** An API that supports interaction between third-party solutions and the Operations Center server. For more information, see the *Operations Center 5.5 Web Services Guide*.
- **SQL Views.** Allows read access to the Operations Center server. For more information, see the *Operations Center 5.5 SQL Views Guide*.

3.6 Databases for Operations Center

Operations Center stores data in both embedded databases and databases that you create and configure using third-party tools.You'll need to set up and configure the database to handle the following features:

- **Configuration Storage:** define a database for Operations Center configuration data, version tracking, and to control connections to all databases configured for use with Operations Center, including the Event Data Store, Service Warehouse, Configuration Storage.
- **Dashboard:** must be configured to use an external database. See *Operations Center 5.5 Dashboard Guide* for more information and configuration information.
- **Event Data Store:** define a database for SNMP Integrator, Event Manager, and/or alarm suppression.
- **Service Warehouse:** define a database to record alarm history and comments, historical performance and Service Level metrics. For more information about the data stored in the BSW, see the *Operations Center 5.5 Service Warehouse Data Dictionary*.

For these databases, the `/OperationsCenter_install_path/database/samples` directory contains individual directories for each of the supported databases. Within each directory is a *Readme* file that contains suggestions for assigning a default tablespace for managing performance and Service Level

Agreement (SLA) data, suggestions for installing and configuring the database for use with the Service Warehouse, and scripts, which the database administrator should review for compliance and usefulness.

For information about calculating space requirements for the Operations Center database, see the *Operations Center 5.5 Server Configuration Guide*.

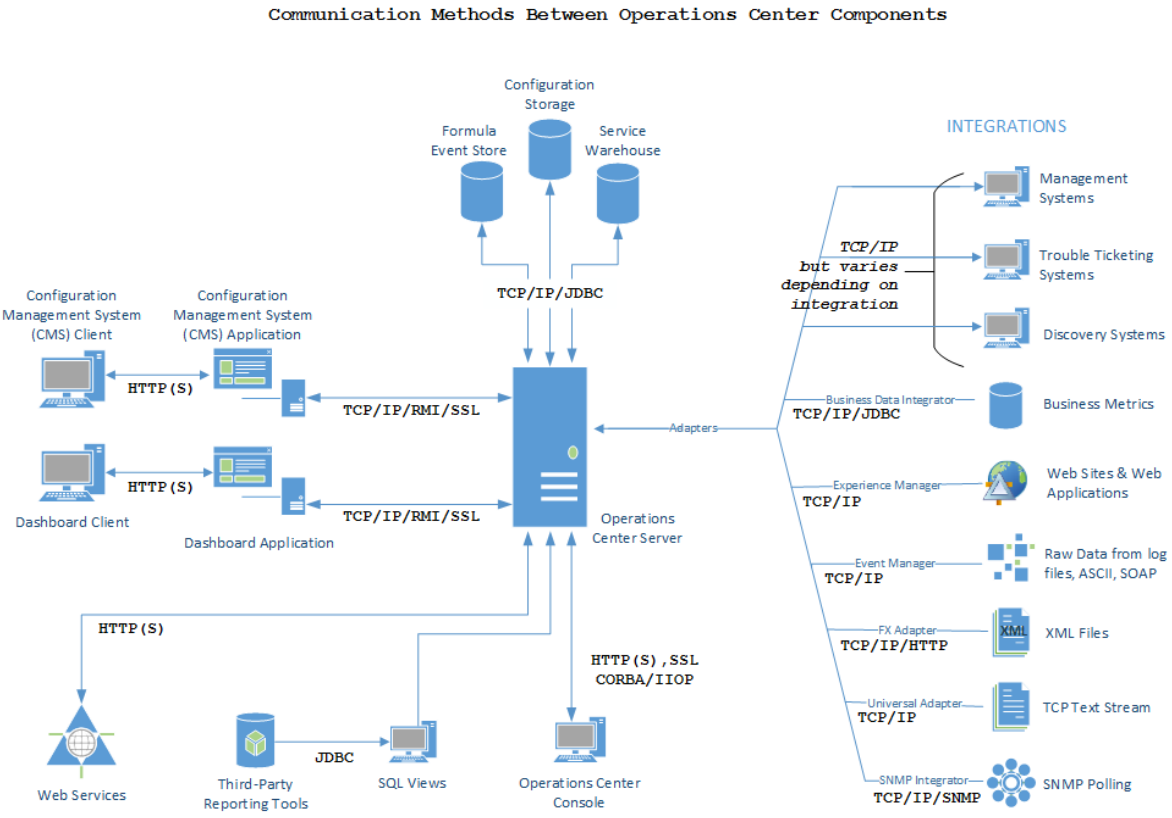
Database definitions, which are managed in the Operations Center console, establish configuration settings and other parameters required to establish a connection between the Operations Center server and the database.

Operations Center also supports connections to an external data source for limited management of service level agreements. For more information, see the *Operations Center 5.5 Service Level Agreement Guide*.

3.7 Communications in Operations Center

Components of the Operations Center solution must communicate and transfer data among each other. The Operations Center server, in particular, must communicate with third-party systems such as management systems as well as clients, databases, and other servers.

Figure 3-2 *Communications between Operations Center components*



Review the following sections to learn how the Operations Center server communicates:

- Section 3.7.1, “Operations Center Server Port Usage,” on page 24
- Section 3.7.2, “Operations Center Server to Management Systems,” on page 24
- Section 3.7.3, “Operations Center Server to Console,” on page 25

- Section 3.7.4, “Operations Center Server to Operations Center Server,” on page 26
- Section 3.7.5, “Operations Center Server to Other Components,” on page 26

3.7.1 Operations Center Server Port Usage

Operations Center uses a range of ports. The specific ports used depends on the overall architecture that is implemented (whether Operations Center is inside/outside firewalls, whether adapters must communicate across firewalls to management systems, and so on), as well as the data source.

During every initialization, Operations Center starts at a specified number (2000 by default) and looks for consecutive range of unused ports equal to the number it needs, up to a specified value (3000 by default). The potential exists for the server to use different ports each time the server starts.

If you need the ports to be specific to meet firewall or other security restrictions, you can change the server configuration to set specific ports. For information, see *Configuring Ports* in the *Operations Center 5.5 Server Configuration Guide*.

3.7.2 Operations Center Server to Management Systems

The Operations Center server receives data from a management system or other Operations Center tool, such as BDI, Experience Manager, Event Manager, or SNMP Integrator, via an adapter. In addition to integrating the data for reporting and monitoring, the Operations Center server has functionality that replicates the functions of the management system.

Each adapter is an API that is written for a specific product and a specific version of that product. For a list of management systems for which Operations Center provides an adapter, see Chapter 4, “Supported Versions and Hardware Requirements,” on page 27.

Each adapter has different requirements from a firewall configuration standpoint. An adapter that uses an ORB connection to a management system has a configurable port, as well as IIOP communication.

A few adapters utilize a specific port, but the actual data transferred is in clear text over a socket connection such as Tivoli T/EC and potentially the Operations Center Event Manager. This can be locked to a specific port, but the protocol can vary.

Review the following sections to understand request brokers and relay connections in Operations Center:

- “Objects Request Brokers” on page 25
- “Secure Relay Connections” on page 25

Objects Request Brokers

Some adapters connect directly to the management system, while others require an additional software component called an Object Request Broker (ORB), which is written in C++ or Java. The ORB provides a CORBA "wrapper" for the management system API or gateway, and in some cases communication between the ORB and Operations Center server is accomplished using the CORBA IIOP. For adapters requiring ORBs and supported platforms, see Table 4-5 on page 33.

Operations Center uses a different mechanism to initiate communication with ORBS, taking advantage of the fact that ORBs wait for the server to initiate contact. General ORB behavior requires two open ports:

- Command-and-control from the server to the ORB
- Unidirectional IIOP from the ORB to the server

Default port numbers are provided for each type of ORB, but can be changed.

Secure Relay Connections

Operations Center provides a secure relay connection for integrating with some third-party management systems. The relay connection provides secure cross-host communication by acting as an intermediary, accepting and delivering messages between the Operations Center server and the third-party management system.

IBM Micromuse Netcool and BMC Software Patrol Enterprise Manager (PEM) are currently supported. For more information on these integrations and on configuration of secure relay connections, see the *Operations Center 5.5 Adapter and Integration Guide*.

3.7.3 Operations Center Server to Console

The Operations Center console uses two ports. Both initial connections are through the HTTP (or HTTPS) port.

The Operations Center server cannot know in advance the location of a Operations Center console (or another server) that wants to communicate with it. For this reason, Operations Center consoles (and other Operations Center servers) issue a standard request to a target server when they want to communicate with it. This request travels over either the unsecured or secured Web port, and takes the form of a special URL. The originating Operations Center console (or server) parses the data returned by this request to determine which port number to use for further communication with the target.

If the Operations Center console contacted the target server using secure HTTP, the port value returned is the bidirectional IIOP port for secure data. If the Operations Center console contacted the target server using unsecured HTTP, then the port value returned is the bidirectional IIOP port for standard HTTP.

The same mechanism used to return port values also specifies the IP address of the server. However, in the presence of a Network Address Translation (NAT) device, the IP address published by the server is the IP address of the server from the private side of the NAT device, not the public side. This IP address does not allow the client to successfully pass from the user's desktop through the NAT device to reach the server. You must make a configuration change to the Operations Center server to account for this behavior. For more information, see the *Operations Center 5.5 Server Configuration Guide*.

3.7.4 Operations Center Server to Operations Center Server

Operations Center allows for data from one Operations Center server to be used by another Operations Center server. The connection is similar to how the Operations Center console connects to a Operations Center server. You can connect multiple Operations Center servers for a cascading effect, but each connection slows performance.

Operations Center servers running the same version can always be connected with each other. However, check the *Release Notes* to verify if Operations Center servers running different versions can communicate over an InterConnection Adapter (ICA), and what versions are supported.

The connection is made using the ICA, which allows data that resides in one Operations Center server (such as Server A) to be visible to and used by another Operations Center server (such as Server B). The servers can be divided by a firewall.

To configure the ICA, you must specify the host name and HTTP port of the Operations Center server to which you want to connect. To secure the connection, you can use HTTPS and restrict access by IP address. For more information, see the *Operations Center 5.5 Server Configuration Guide*.

Data from Server A appears in Server B as local elements, which can be used to build service models. The state (such as current condition) is propagated to elements in service models. You can also create local service level agreements (SLAs) on these elements. Any SLAs that apply to the element on Server A appear as remote SLAs on Server B. For more information on service models and SLAs; see the *Operations Center 5.5 Service Modeling Guide* and *Operations Center 5.5 Service Level Agreement Guide*, respectively.

3.7.5 Operations Center Server to Other Components

The Operations Center server also communicates with other servers, such as the Web server and Image server, and databases.

When configuring the Operations Center server, you must specify the database for the Configuration Storage data source and the settings (such as Java runtime and trace levels) for connection to the databases. You must also specify the port for connection to SQL Views (if that product is used).

Database connections most likely use a specific port, but the communications is usually through a JDBC protocol. Depending on the JDBC driver, it might be pure JDBC or a vendor-specific protocol, such as SQL*Net or DBLib, and so on.

You must also define the ports for communication with the Web server and Image server. Communication with the Web server can use either HTTP or HTTPS.

RMI communications can be used between the Operations Center server and Web server used for the dashboard. RMI is the Remote Method Invocation, which is a Java application programming interface used for communication using HTTPS.

The dashboard's Web server also supports the use of a truststore a (defined as a repository for keys that are trusted by the Operations Center server or the dashboard server) and a keystore (defined as a repository for certificates that the Operations Center server or dashboard server uses to identify itself). Any certificate that is in the truststore, or signed by a certificate in the truststore, is trusted by the server. Operations Center validates the certificate dates.

The certificate used to secure HTTP communications on the Operations Center server or dashboard server must also be used to secure RMI communications on that server. If your environment requires different certificates for RMI communications, contact Support (https://www.netiq.com/support/) for assistance.

4 Supported Versions and Hardware Requirements

This section provides details on hardware requirements and information on specific operating systems, client platforms, databases and third-party applications and tools that are supported for use with Operations Center.

Performance will vary based on the configuration and data of your implementation, including but not limited to:

- hardware, database selection and configuration, management systems and integrations
- rate, volume and size of events and data stored
- custom scripts, integrations, operations, and user-applied changes
- size and complexity of service views
- complexity of SLA definitions and Dashboard views

Contact Consulting (https://www.netiq.com/consulting/) for assistance with planning your implementation.

NetIQ provides various levels of support for specific versions of operating systems, client platforms, and databases; as well as for integrations to third-party management systems, discovery tools and trouble ticket systems:

- **Tier 1 (Certified):** NetIQ certifies the use of and supports all operating systems, databases, hardware, and third-party integrations as specified.
- **Tier 2 (Best Level):** NetIQ provides a best level effort of support for:
  - The next newest version of Tier 1 supported operating systems, client platforms, databases, and third-party integrations.
  - The previous version of Tier 1 supported operating systems, client platforms, databases, and third-party integrations.

  If Support is unable to resolve an issue in a reasonable amount of time as determined by Support, you must migrate to a Tier 1 certified version or work with Consulting (https://www.netiq.com/consulting/).
- **Tier 3 (Community-Driven):** NetIQ does not provide support for:
  - Any integrations not provided as a part of the official Operations Center product release. This includes any adapters or integrations built by customers, Consulting, or NetIQ partners.

  When attempting to use Operations center with any of the above, we suggest researching or posting the issue on the Community Forum (https://forums.netiq.com/forumdisplay.php?26-Operations-Center); or contacting a NetIQ partner or Consulting (https://www.netiq.com/consulting/).

Review the following sections for information on the supported software and hardware:

4.1 Operating Systems

Table 4-1 details the platforms that the Operations Center server and components are validated to install and run on.

Operations Center requires a 64-bit Virtual Machine because of the memory demands of the application.

Table 4-1 *Supported Operating Systems by Product Component*

Operating System	Operations Center Server	Dashboard	CMS
Microsoft Windows Server 2008 (64-bit and R2) and 2012.	X	X	X
SUSE Linux Enterprise Server 11 x86 (64-bit)	X	X	X
Red Hat Enterprise Linux (RHEL) 5, 6.2	X	**6.2 only**	**6.2 only**
Sun Solaris 10 on Sparc and x86	X	X	X

If installing the Operations Center server, Dashboard or CMS on Windows 2012 using a DVD/CD, Mounted ISO , or Mounted Network install; you will need to modify the property settings of the respective `install.exe` file t to run the program in compatibility mode for Windows 7. See the installation instructions in *Operations Center 5.5 Server Installation Guide*, *Operations Center 5.5 Dashboard Guide*, and *Operations Center 5.5 Configuration Management System (CMS) Guide* for further details.

The following section provides details on Java Runtime Environment requirements:

4.1.1 Java Runtime Environment

Operating system patches must be applied to ensure they comply with Java 1.7.0_60 Runtime Environment (J2RE), which is the version currently supported. Contact the appropriate JRE vendor to obtain patch information for each operating system.

JRE 1.7.0_60 is automatically installed with Operations Center on Windows 64-bit and R2.

For all Unix operating systems, you must download and install a compatible version of the JRE prior to installing Operations Center. The JRE must be part of a JDK. You can use a different JRE; however, you might be required to install 1.7.0_60 if you encounter problems.

When installing a Java Virtual Machine (JVM) other than that provided by Operations Center), you must install a Java Development Kit (JDK) as the JRE-only Installation for Windows does not contain the server libraries that are required to run the Operations Center server with a `-server` option.

Table 4-2 details the Java Runtime Environment versions that are validated for use with Operations Center for each operating system. Note that the Operations Center SNMP adapter is supported for the Oracle JDK only.

Table 4-2 *JREs Validated for use with Operations Center*

Operating System	Operations Center JRE Version	Vendor
Linux	1.7.0_60	IBM, Oracle (formerly Sun)
Solaris	1.7.0_60	Oracle (formerly Sun)
Windows	1.7.0_60	Oracle (formerly Sun)

If you are installing Operations Center on a 64-bit host, you must download and install the appropriate 64-bit JDK prior to installing Operations Center. When installing Operations Center, point the installer to the downloaded JDK that contains the JRE. Later, this can be reconfigured in the Operations Center Configuration Manager.

If installing the Dashboard on Solaris x64, be sure to modify the Apache `Setclasspath.sh` file to reference the Java path in your AMD64 installation in order for the Dashboard to start successfully. For example, `_RUNJAVA="/usr/jdk1.7.0_60/jre/bin/amd64/java"`

To download a compatible JRE, contact the appropriate vendor and follow the necessary instructions from the vendor to install the JRE. Appropriate patches must be applied to the operating system you are running to make it compatible with the JRE.

When running Java 7 on a Windows server, it is necessary to have the `msvcr100.dll` file in your WINDOWS\System32 directory for Operations Center server to run successfully as a service. To obtain the `msvcr100.dll` file, download and install the Microsoft Visual C++ 2010 Redistributable Package from the Microsoft Web site:

- **x86:** Download the Microsoft Visual C++ 2010 Redistributable Package (x86)
- **x64:** Download the Microsoft Visual C++ 2010 Redistributable Package (x64)

4.2 Client Platforms

Operations Center supports:

- Microsoft Internet Explorer 10, 11

  (Adobe SVG Plug-in is required to access some features in the Operations Center Dashboard.)
- Mozilla Firefox
- Google Chrome

Any machine on which the Operations Center console is run must be connected to the Internet or the corporate Intranet and meet the following minimum requirements:

- **Free Disk Space:** 200 MB
- **Memory Allocation Space (RAM):** 2 GB RAM
- **CPU (UNIX):** 500+ MHz
- **CPU (Windows):** 1 GHz

The above requirements are general guidelines. Your requirements might vary depending on your implementation. Please work with NetIQ Consulting to determine the minimum requirements based on your implementation.

4.3 Databases

The following sections provide information about supported database management systems for Operations Center components, embedded databases, and JDBC driver support for Data Integrator deployments:

- Section 4.3.1, "Supported Databases," on page 30
- Section 4.3.2, "Embedded Databases for Dashboard, SQL Views, and Operations Center Server," on page 31
- Section 4.3.3, "JDBC Support in Data Integrator," on page 31

4.3.1 Supported Databases

Supported database management system version are outlined in Table 4-3 by Operations Center component. Application performance varies depending on the underlying database architecture. For assistance in selecting the most efficient database for your implementation, contact NetIQ Consulting.

Table 4-3 *Supported Management Systems by Product Component*

DBMS	Configuration Storage*	Service Warehouse & Event Data Store**	Version Tracking	Dashboard	Event Manager	Experience Manager
IBM DB2 9.7	X	X				
Microsoft SQL Server 2008, 2012	X	X	X	X	X	X

DBMS	Configuration Storage*	Service Warehouse & Event Data Store**	Version Tracking	Dashboard	Event Manager	Experience Manager
Oracle 11g, 12c	X	X	X	X	X	X
PostgreSQL 9.3.4	X	X	X			
Sybase ASE 15.7	X	X**	X			X

*The database used for Configuration Storage must be case insensitive.

**The Event Data Store for use with SNMP Integrator and Alarm Suppression only. See Event Manager column for supported databases with that use case. Note that Alarm suppression is not supported on Sybase.

4.3.2 Embedded Databases for Dashboard, SQL Views, and Operations Center Server

Table 4-4 lists products that have embedded databases installed as part of the product installation.

Table 4-4 *Embedded Databases*

Product	Installs with…
Dashboard	HypersonicSQL database to store portlet and configuration information. It is necessary to configure the dashboard to use Oracle or SQL Server. For more information about configuring a database for the dashboard, see the *Operations Center 5.5 Dashboard Guide*.
SQL Views	Apache Derby, a relational database implemented entirely in Java. Note that Apache Derby only supports DB2 ODBC drivers version 9 and below.
Operations Center Server	Object ODB which can be used for the Configuration Storage database.

4.3.3 JDBC Support in Data Integrator

Data Integrator features and functionality are fully supported. Because each deployment is end-user specific, a best level effort of support is provided on JDBC issues and definition deployments.

The Data Integrator supports JBDC drivers in general. Connection templates are provided for the following commonly used databases:

- Apache Derby
- IBM DB2
- JTDS
- MS SQL Server
- MySQL

- Oracle
- Postgres
- Sybase
- Sybase JConnect

4.4 Hardware Requirements

The Operations Center server must be installed on a server-class machine that supports the specified Java environment and one of the specified operating systems.

At a minimum, 8 GB RAM for 64-bit and a dual-processor are needed, but more RAM might be required as memory and processing speed requirements depend upon your configuration, particularly the number of systems and amount of data being integrated into Operations Center. Therefore, it is necessary to tune the JVM memory settings based on your usage and environment. For help on determining more specific hardware requirements, contact Consulting.

For more information regarding memory requirements and configuration, see the *Operations Center 5.5 Server Installation Guide*.

Disk space requirements vary based on the size and configuration of your environment. Below are minimum disk space estimates for the Operations Center server and components.

- 2 GB for the Operations Center server
- 650 MB for the Operations Center configuration storage database (estimated growth rate will vary based on product usage)
- 1.5 GB for the Operations Center Dashboard
- 100 MB for the Dashboard database (estimated growth rate will vary based on product usage. For example, an average is likely 30 MB per community)
- 30 GB for the Operations Center Experience Manager

If you need help determining more specific disk space requirements, contact Consulting.

4.5 Third-Party Integrations

4.5.1 Applications and Management Systems

For more information about integrating to these applications and management systems, see “Application and Management System Integrations” in the *Operations Center 5.5 Adapter and Integration Guide*.

Tier 1 Application and Management Systems

Table 4-5 provides a list of all Tier 1 supported Application and Management Systems.

Table 4-5 *Supported Application and Management System Versions*

Application/Management System	Tier 1 Supported Versions	Notes
Amazon Elastic Compute Cloud (Amazon EC2)	July 2010	
BMC Software Event Manager/Impact Manager	7.2, 9.0	Supported ORB platforms: ◆ AIX ◆ HP-UX(PA-RISC Only) ◆ Solaris ◆ Windows 2000
BMC Software PATROL	BMC PATROL 7.5 Agent 3.5	
BMC Software PATROL Enterprise Manager (PEM)	4.3	
Castle Rock Computing SNMPc	7.0.19	
CiscoWorks2000 Device Fault Manager	2.0, DFM 2.06 (based on LMS 2.6)	
Computer Associates (CA) Spectrum	9.0, 9.2, 9.3	CA Spectrum 9.3 requires the Operation Center server to be running JRE 1.7.
Computer Associates Unicenter	3.1, R11 (for TNG or NSM products)	Supported ORB platforms: ◆ Windows 2000
EMC SMARTS	8.1, 9.2	The EMC SMARTS 9.2 adapter is only compatible with 64 bit Operations Center servers.
HP OpenView Network Node Manager	7.5.1	Supported ORB platforms: ◆ HP-UX(PA-RISC Only) ◆ Solaris ◆ Windows 2000 ◆ RedHat Linux
HP OpenView Network Node Manager i-series	8.1	Requires the NNMi SDK Enablement license from HP.
IBM Micromuse Netcool	7.4	
IBM Tivoli Enterprise Console (T/EC)	3.9	Supported ORB platforms: ◆ AIX ◆ HP-UX(PA-RISC Only) ◆ Solaris ◆ Windows 2000 ◆ RedHat AS 2.1, 3.0

Application/Management System	Tier 1 Supported Versions	Notes
IBM Tivoli Enterprise Console (T/EC)+, Database Edition	3.9	
IBM Tivoli NetView	7.14	Supported ORB platforms: ◆ AIX ◆ Solaris ◆ Windows 2000
Microsoft Operations Manager (MOM) and Microsoft System Center Operations Manager (SCOM)	MOM 2005 SCOM 2007, 2012	
NetIQ AppManager	7.0.4, 8.0, 8.2	
NetIQ AppManager Control Center	7.0.4, 8.0, 8.2	
NetIQ Sentinel	6.1, 7.0.1, 7.1.1.2	
Novell Cloud Manager	2.0, 2.1	
Novell ZENworks Configuration Management	11	
PlateSpin Orchestrate	3.2	
SolarWinds Orion	10.7	

Tier 2 Application and Management Systems

The following application and management systems are no longer listed as Tier 1 supported products but are still available for Tier 2 support:

- Blade Logic Operations Manager, v2005
- Cisco Info Center (CIC), v3.7
- EMC SMARTS, v7.1
- HP Openview Operations for UNIX, v8.*x*

  Supported ORB platforms are HP-UX (PA-RISC Only) and Solaris
- IBM Micromuse Netcool, v7.3
- Novell ZENworks Linux Management, v7.3
- SolarWinds Orion 9.5

Support might require remote access to your environment.

4.5.2 Discovery Tools

For more information about integrating to these discovery tools, see "Discovery Tool Integrations" in the *Operations Center 5.5 Adapter and Integration Guide*.

- "Tier 1 Discovery Tools" on page 35
- "Tier 2 Discovery Tools" on page 35

Tier 1 Discovery Tools

Table 4-6 provides a list of all Tier 1 supported discovery tools.

Table 4-6 *Supported Discovery Tool Versions*

Discovery Tool	Tier 1 Supported Versions	Notes
IBM Tivoli Application Dependency Discovery Manager (TADDM)	7.2.0.x	
PlateSpin Recon	3.6	

Tier 2 Discovery Tools

The following discovery tools are no longer listed as Tier 1 supported products but are still available for Tier 2 support:

- IBM Tivoli Application Dependency Discovery Manager (TADDM), v7.1.2
- Mercury Application Mapping, v5.0
- Symantec Clarity, v4.0
- Tideway Foundation, v7.2

Support might require remote access to your environment.

4.5.3 Trouble Ticket Systems

For more information about integrating to these applications and management systems, see "Trouble Ticket Systems Integrations" in the *Operations Center 5.5 Adapter and Integration Guide*.

- "Tier 1 Trouble Ticket Systems" on page 35

Tier 1 Trouble Ticket Systems

Table 4-7 provides a list of all Tier 1 supported trouble ticket systems.

Table 4-7 *Supported Trouble Ticket Systems Versions*

Trouble Ticket System	Tier 1 Supported Versions	Notes
HP ServiceCenter	6.2	
HP Service Manager	7, 9.3	
BMC Remedy ARS	7.2, 8.1	

4.6 Requirements for the Dashboard and CMS

The Dashboard and CMS are both Web-based applications. Both require access to the Operations Center server. While they can be installed on the same server as Operations Center, they do not need to be on the same host machine.

For more information, see the *Operations Center 5.5 Dashboard Guide* or *Operations Center 5.5 Configuration Management System (CMS) Guide*.

Table 4-8 lists the deployment notes for the Dashboard and CMS:

Table 4-8 *Dashboard and CMS Requirements*

Host Server	For supported platforms, see Section 4.1, "Operating Systems," on page 28. For databases, see Section 4.3, "Databases," on page 30. The Dashboard/CMS server must have: ◆ JDK 6.0 or higher. For more information, see Section 4.1.1, "Java Runtime Environment," on page 29. ◆ Environment variable called %JAVA_HOME% in Windows or $JAVA_HOME in Linux/Unix set to point to your JDK directory. For the Web/Image Server, the Apache Tomcat requirements are: ◆ The Dashboard installs with Apache Tomcat v6.0.37 and Image Server ◆ CMS installs with Apache Tomcat v6.0.37
Deployment	The Dashboard, CMS, and Operations Center be at the same Operations Center patch release. When installed on a different physical server than the Operations Center server, the Dashboard/CMS server must resolve to the Operations Center server for communications.
Operations Center Server	For CMS, Version Tracking must be configured on the Operations Center server. For more information, see *Operations Center 5.5 Version Tracking Guide*.
User Access	Users must use a Web browser to access the Dashboard and CMS. For supported browsers, see Section 4.2, "Client Platforms," on page 30. Web browsers must be configured to allow Active X controls. If the correct plug-in is not installed, you are prompted to install it. To access the Dashboard Layout and ChartBuilder (Internet Explorer only) portlets , the Adobe SVG Viewer 3.0 must be installed on the user's machine.
Additional Information	The Dashboard is compatible with portlets that are JSR-286 compliant. Any portlet that uses this standard can be deployed in the Dashboard.

NOTE: NetIQ provides support for Operations Center portlets only. The Dashboard leverages portlets from third-party sources including Liferay v.5.2.3. For support for any third-party portlets, contact the vendor that provided the portlet.

Because the Operations Center Dashboard offers flexibility to design your own dashboards, it might be necessary to upgrade hardware, increase memory allocations, alter page designs (including number of charts or expressions on a chart), or limit the amount of users to achieve optimal

performance. Performance varies based on the number of users, complexity of installation, and amount of data in your dashboard pages. We suggest you contact consulting for help in implementing a high performing solution.

4.7 Requirements for Experience Manager

The Experience Manager Monitor is validated to install and run on the same platforms as the Operations Center server.

Any machine on which the Experience Manager is run must be connected to the Internet or the corporate Intranet and meet the following minimum requirements:

- **Free Disk Space:** 30 GB
- **Memory Allocation Space (RAM):** 1 GB RAM
- **CPU:** 2+ GHz

Actual requirements can vary depending on the types of tests setup, the amount of users being simulated, thread counts, etc. NetIQ Consulting can provide a recommendation after understanding the environment and setting up some test cases.

For more information about the Experience Manager, see the *Operations Center 5.5 Experience Manager Guide*.

4.8 Section 508 Compliance Summary

Section 508 requires that Federal agencies' electronic and information technology is accessible to people with disabilities. Operations Center solutions strive to provide a Web Dashboard that is accessible to every person, including people with disabilities.

Section 508 defines 16 Web Standards (1194.22 A-P) and 12 Software Standards (1194.21 A-L). The majority of Operations Center Dashboard portlets are evaluated against all 16 Web standards and only 2 Software standards (as the other Software Standards are not applicable).

The 508 compliance and compatibility for Operations Center Dashboard components are outlined in Table 4-9.

Table 4-9 *Dashboard Component 508 Status*

Dashboard Component	508 Status
Alarms Portlet	Compatible*
Chart Builder	Compliant
Element Properties Portlet	Compliant
Information Portlet	Compatible*
Layout Portlet	Compliant
Navigation Portlet	Compliant
Performance Portlet	Compliant
Refresh Portlet	Compliant

Dashboard Component	508 Status
Root Cause Portlet	Compliant
Status Portlet	Compliant
SLA Compliance Report	Compatible*
SLA Status Report	Compliant

* Only three of the Operations Center Dashboard portlets have failed to qualify for compliance, being non-compliant in only 1 or 2 accessibility items out of the 14 applicable items.

Our products are constantly being tested and improved for Section 508 compliance. Any non-compliance is logged into our tracking system to be addressed. For more information about our current compliance status, please contact Support (https://www.netiq.com/support/).

Enabling 508 accessibility in the Operations Center Dashboard requires some configuration by the Operations Center administrator. For instructions, see "Enabling the Dashboard for Section 508 Accessibility" in the *Operations Center 5.5 Dashboard Guide*.

5 Operations Center Deployment Planning

Now that you know what Operations Center can do, you need to plan how to make the Operations Center solution work within your organization. The resources needed depend upon the tools and components that you opt to use.

There are three areas that you need to consider:

- Section 5.1, "Data Inventory," on page 39

  What data do you want to integrate into Operations Center?
- Section 5.2, "End User Requirements," on page 44

  Who will be using the data, for what, as well as how they should access it?
- Section 5.3, "Resource Distribution," on page 44

  After you have determined the tools and their components that you will use, you should ensure that you have the resources to support them.

When you are ready to install and configure your Operations Center implementation, use the "Implementation Checklist" as a guide to walk you through the process. It has links to the documentation guides that provide additional information for each feature.

5.1 Data Inventory

To determine what data you want to integrate, you need to identify the data you need, then consider how the systems from which data is collected are organized and should be integrated into Operations Center. You also need to make sure that you have information from the third-party management systems and other tools from which you are integrating data.

- Section 5.1.1, "Identify Needed Data," on page 40
- Section 5.1.2, "Organize Systems," on page 41
- Section 5.1.3, "Note System Information," on page 43

5.1.1 Identify Needed Data

To identify the data that you want to integrate into Operations Center, consider that Operations Center relates business services to IT resources. Data is used in Operations Center as elements that represent objects or processes within your business services.

Most business services rely on a standard set of IT resources, summarized in Table 5-1:

Table 5-1 *Business Service Resource Components*

Category	Monitored Objects	Explanation
Network	Routers, switches, Virtual Private Networks, ports, and so on	The paths that exist between the enterprise management platforms and the servers where the application components exist.
Users	Workstations, routers, switches, Virtual Private Networks, ports, and so on	The devices and paths that allow users to connect to an application front-end (such as, Web server).
Servers	CPU, memory, and file system space utilization, and so on	Includes the servers on which application processes run, as well as other servers upon which an application might be dependent.
Applications	Running processes, services, tasks, and so on	Processes and services that must run to drive an application.
Databases	Database tables, locks, database processes and services, and so on	Also monitors the processes, services, and servers that support the database itself.

After identifying the IT and enterprise resource components, perform a Business Process Analysis (BPA) to identify all the business management systems that provide information about them.

If you are missing any data, consider how to capture. A Operations Center tool used for integration, such as Business Data Integrator or Event Manager, might be able to capture the data you need. Or, you might need to consider implementing additional third-party management systems.

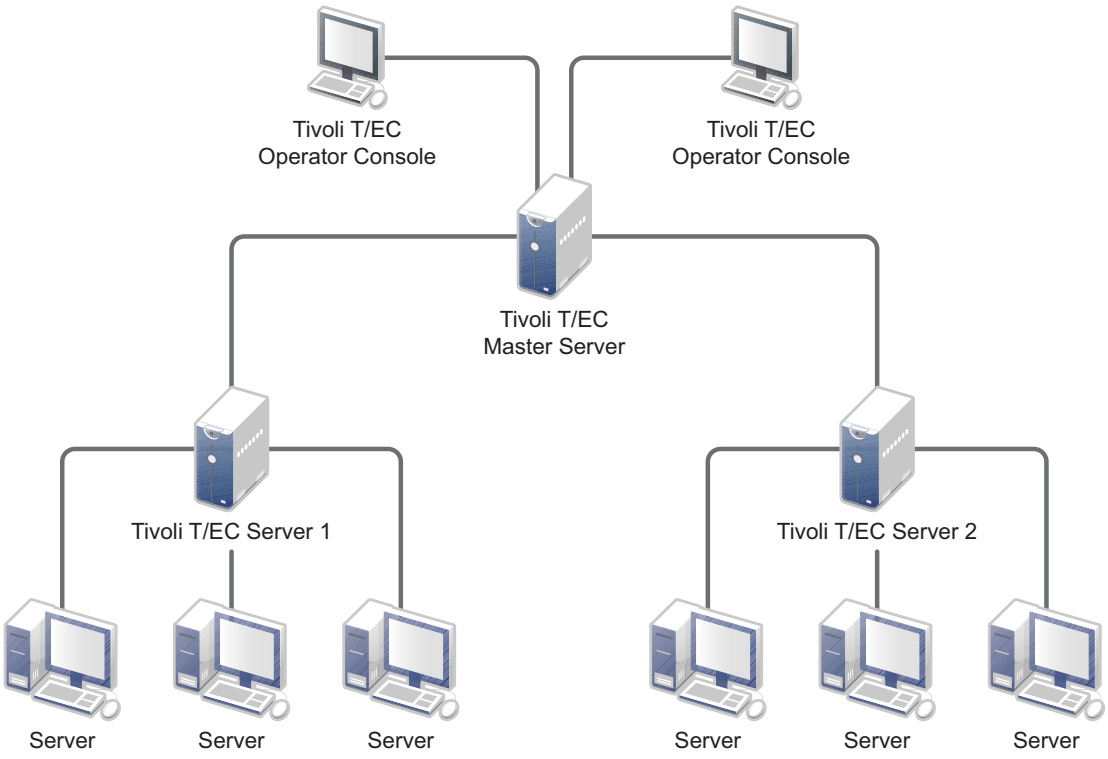
5.1.2 Organize Systems

To integrate data into Operations Center server, you should consider how your management systems are deployed.

You can have multiple installations of the same management system because the tool is monitoring specific areas, or because it is deployed using multiple instances of the management platform. In some cases, you can connect to a top-level system or replace the top-level system with Operations Center.

Figure 5-1 shows a sample Tivoli T/EC environment with multiple T/EC systems:

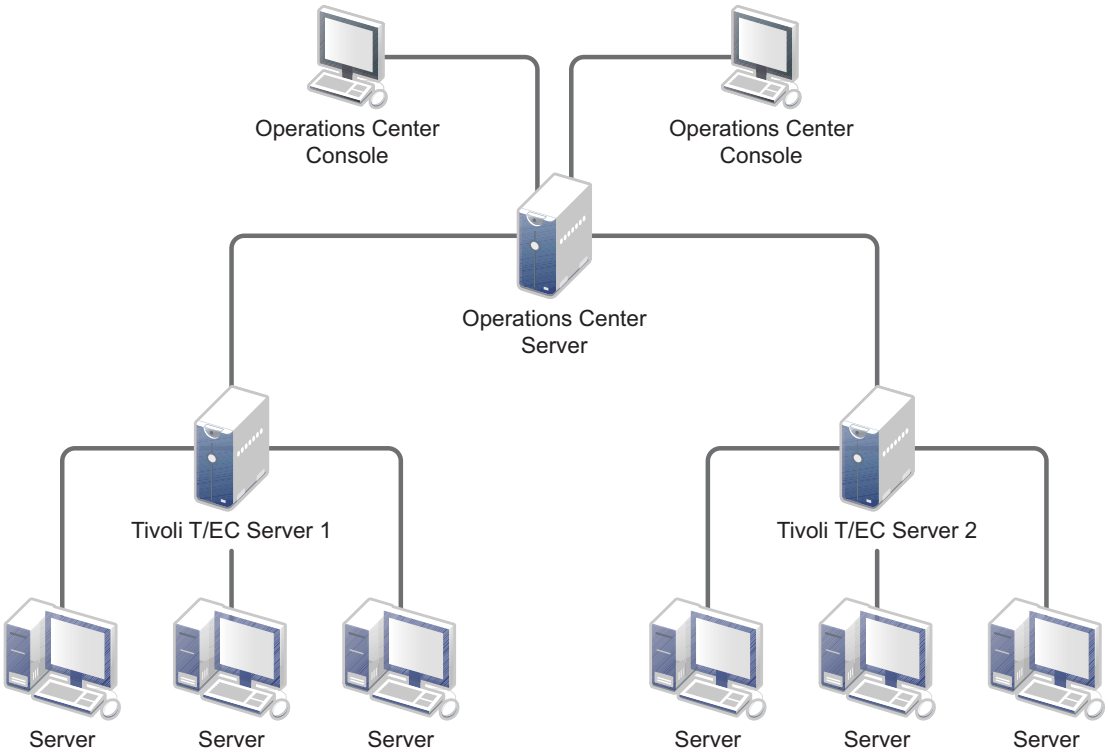
Figure 5-1 *Tivoli T/EC Environment with Multiple T/EC Systems*



In this example, T/EC Server 1 monitors a specific group of servers and T/EC Server 2 monitors other servers. A master T/EC Server rolls up the data from the two T/EC Servers.

One option for integrating the T/EC systems with Operations Center is to replace the T/EC Master Server with a Operations Center server as shown in Figure 5-2:

Figure 5-2 *Replacing the T/EC Master Server with a Operations Center server*

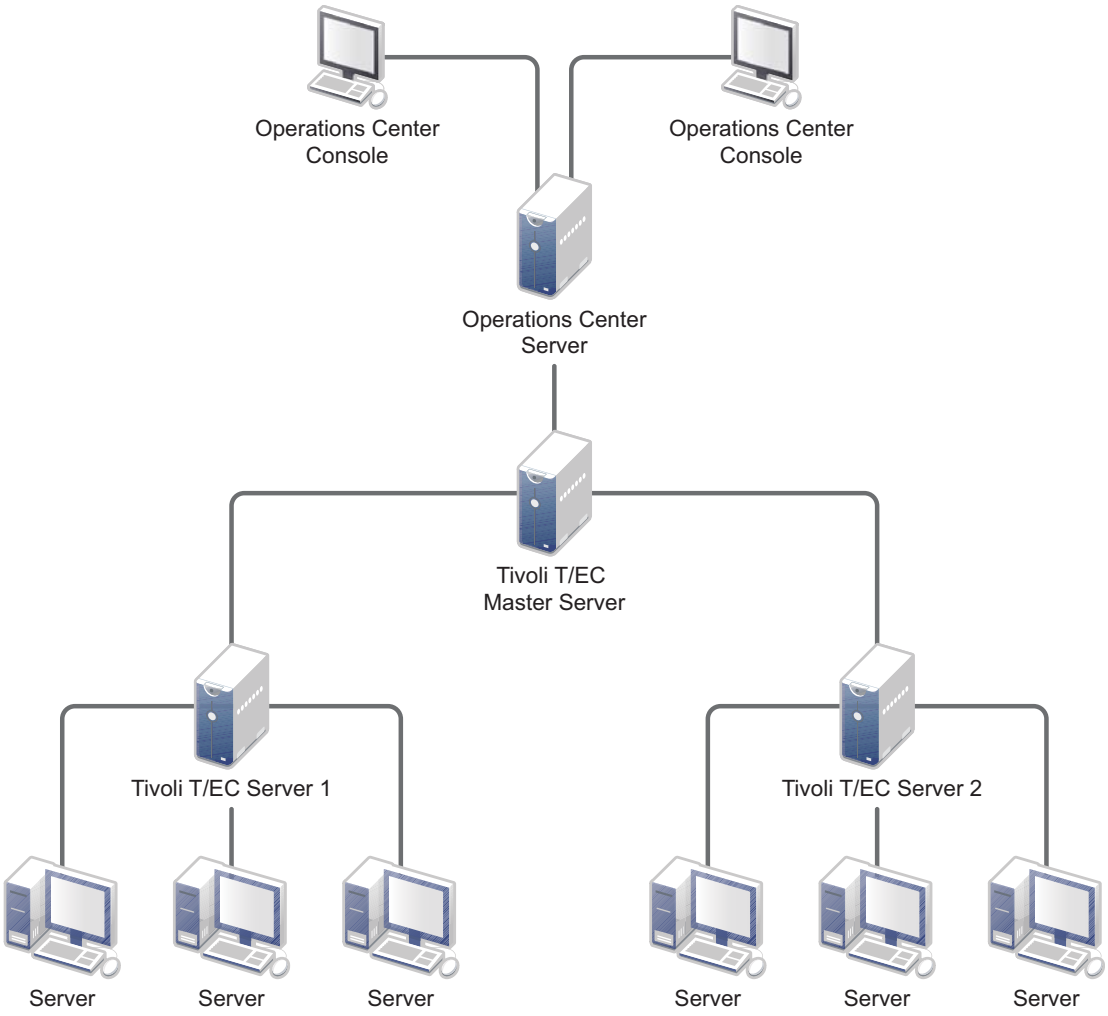


In this option, each server communicates directly with the Operations Center server. You should define two adapters in the Operations Center console to account for each of the T/EC Servers.

If additional rules processing or correlation takes place in the Master T/EC Server, do not replace it with the Operations Center server. Instead, exercise the second option for integrating these systems.

The second option is to have the Operations Center server communicate with the Master T/EC Server as shown in Figure 5-3:

Figure 5-3 *Operations Center server Communicating with the Master T/EC Server*



In the second option, Operations Center server communicates only with the Master T/EC Server, so you only need to define one adapter to it in the Operations Center console.

5.1.3 Note System Information

The process of connecting Operations Center to a management system relies on an understanding of the following elements of your environment:

- Management system vendor and version
- IP address, host machine name, network route of the system
- Any network firewalls between management systems
- Login user names, passwords, repository names, and so on

This information is required for defining adapters in the Operations Center console for integration. Details vary based on the type of management system.

5.2 End User Requirements

An important aspect of deploying the Operations Center solution involves who is going to actually use it and what do they need. Consider the following questions:

- **Who are your end users?** Will operators who currently manage data from third-party management systems use Operations Center? Will managers of service level agreements use the SLA management tools? Do executives need a reporting tool?
- **What functionality do they need?** The functionality needed depends upon the user's role in the organization. Operators who actively manage and administer systems should be able to do operations on alarms. Managers who administer service level agreements should be able to create and manage SLAs. Executives who monitor data, whether alarms or SLAs, will need reporting capabilities.

  For more information on functionality in Operations Center, see Chapter 2, "Managing Your Technology and Services with Operations Center," on page 9.
- **How will they access data from the Operations Center server?** How to access data is dependent upon the function that the user wants to accomplish. For monitoring and operations, the user could use either the Operations Center console or the dashboard. For reporting, users can use the dashboard.

  For more information, see Section 3.2, "Operations Center Tools," on page 15.
- **When must the Operations Center server be available?** Typically, applications used by large numbers of employees in a corporation require a high level of availability. Applications with a smaller user base can require a high level of availability based on the profile of the typical application user.

  For example, a smaller user base of executives, partners in a company, or customers could require maximum system availability. These users would find it unacceptable to have no access to the system in the event of a hardware or software failure until the problem is resolved.
- **How quickly do users need data?** Of course, everyone wants everything as fast as possible. You should consider how quickly users must realistically access Operations Center and balance those needs with the costs of the systems and infrastructure needed to promote faster access.
- **How will you ensure that data is protected?** No user wants to lose any important data. So you should consider back ups for Operations Center server. You also should consider security to protect data from unauthorized users. For more information on security in Operations Center, see the *Operations Center 5.5 Security Management Guide*.

5.3 Resource Distribution

After you have determined what data you will collect and who will use the data, you should consider how to distribute the data among different resources. In particular, you should consider how to distribute the data collected for alarm historical and historical performance and service level agreements. This data is stored in the Service Warehouse. In addition, a license to the Operations Center Service Level Manager (SLM) is needed to manage and administer data related to service level agreements (SLAs).

For more information on SLM and SLAs, see the *Operations Center 5.5 Service Level Agreement Guide*.

Access to the Service Warehouse and alarms history data can be achieved in a distributed or centralized environment. InterConnection adapters are required to connect multiple Operations Center servers.

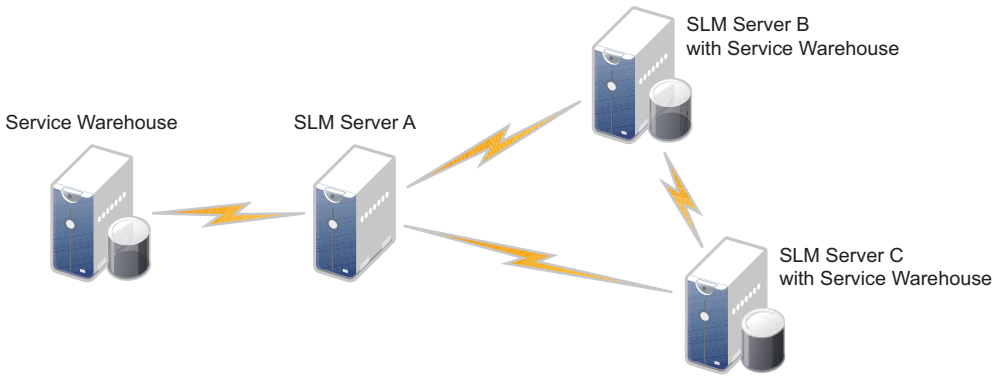
For more information on how to configure InterConnection adapters, see the *Operations Center 5.5 Adapter and Integration Guide*.

- Section 5.3.1, "Distributed Environment," on page 45
- Section 5.3.2, "Centralized Environment," on page 46

5.3.1 Distributed Environment

In a distributed architecture, the workload to monitor and store alarms history can be distributed to multiple Operations Center servers. Distributed historical data can be accessed from any Operations Center server with an InterConnection adapter by using service models that contain elements from the InterConnection adapters (from the remote servers).

Figure 5-4 *Distributed Historical Data Configuration*



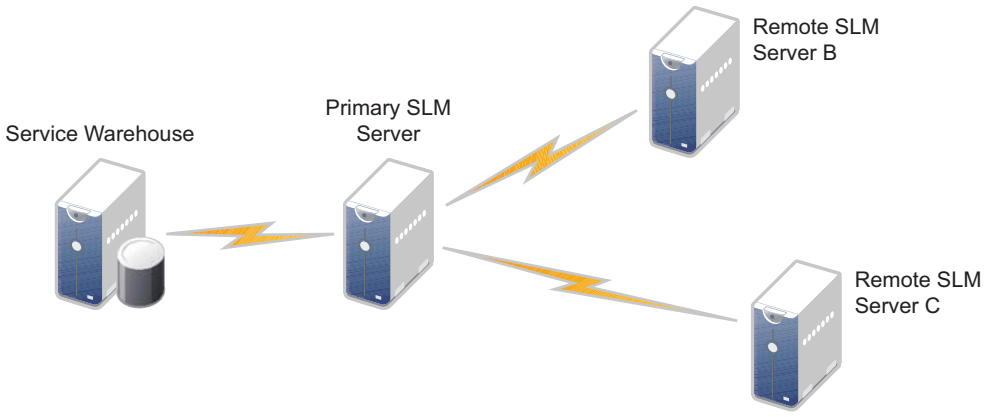
In order to monitor and manage historical performance and SLA data for elements on these remote servers, it is necessary to deploy SLM on each remote server that needs to monitor and manage historically.

InterConnection adapters are then configured to connect pairs of SLM servers. Each SLM server stores historical performance and SLA data locally to establish distinct SLAs and store historical performance and SLA data for each SLM server independent of all other SLM and/or servers.

5.3.2 Centralized Environment

For centralized SLA monitoring and management, you should establish SLAs on a primary server while leveraging the InterConnection adapter connections to centrally establish SLAs on remotely monitored data.

Figure 5-5 *SLA Configuration*



Access to historical performance and SLA data from remote SLM servers requires users to connect directly to the SLM server where data is stored, or connect to that server via its portal.

6 Environmental Considerations

After you have determined the tools and their components that you will use, you should consider how it fits within your existing environment. Consider the following factors:

- Availability
- Speed
- Fault Tolerance
- Firewalls

Different hardware and software configurations can be put into place to achieve the goals for each of these factors. One overriding factor in any configuration choice is obviously cost. You should compare your requirements to your budget to ultimately determine the configuration that you implement.

To understand these environment factors, review the following sections:

- Section 6.1, “Availability and Fault Tolerance,” on page 47
- Section 6.2, “Speed,” on page 50
- Section 6.3, “Firewalls,” on page 50

6.1 Availability and Fault Tolerance

Some terms commonly used to describe a system’s maximum availability are: “24 (hours) by 7 (days),” “three-nines,” or “five-nines,” which describe the required percentage availability (99.9% or 99.999%).

High availability conveys the importance of keeping the system up and running as long as possible. High availability typically refers to the running state of an application. For Operations Center, it generally refers to the whole system as an entity that is available.

High availability has costs associated with it. For example, a system that can be down for 20 minutes for unscheduled outages during a week obviously costs less than one that can be down for 20 minutes over an entire month.

High availability is directly connected to fault tolerance. Fault tolerance usually indicates there is a system in place to ensure undisrupted system availability in the event of hardware or software failure. The type of fault tolerance employed determines the impact on availability if a component of the system fails.

The levels of fault tolerance vary. For example, mirrored drives are good; mirrored RAID drives are better; and dual servers with mirrored RAID drives are even better. Each step in improvement has a cost associated with it.

High Availability can be achieved using hardware and/or software. Some software is provided directly by the hardware manufacturer, while other technologies are add-ons from third parties (hardware and/or software).

To implement high availability and fault tolerance, you should focus on these components:

- Operations Center server
- Management systems that integrate with Operations Center
- Databases used by Operations Center for storing or obtaining data
- Networking components (LAN and/or WAN)

A configuration that achieves high availability can include:

- Dual (or more) servers for Operations Center (physical or clustered)
- Dual (or more) management systems (OpenView, Netcool, etc.; physical or clustered)
- Potentially dual networking components

Review the following sections for more information on server configurations:

- Section 6.1.1, "Operations Center server Configurations," on page 48
- Section 6.1.2, "Example," on page 49

6.1.1 Operations Center server Configurations

The Operations Center server can be configured as either a stand alone server or a clustered server. Each option has an impact on high availability and fault tolerance as follows:

- **Stand alone:** Stand alone is the most basic server configuration. Implementing a single Operations Center server on a RAID volume with a UPS is a simple stand alone system that does not meet the goals of high availability or fault tolerance. A software failure, motherboard failure, or network card failure makes the service unavailable to end users. The service continues to be unavailable until the problem is resolved.
- **Clustered:** Clustered server configurations refer to multiple servers configured in the same way to provide the same type of service, with a single "front door" component that makes it seem a single server. From the backend, only one server provides the service. If the server fails, a second server begins providing the service. The main benefit is end users do not need to reconfigure or reconnect to the server or service, and it often appears as if the service never failed.

Cluster solutions can be both hardware and software based. Software based solutions typically configure multiple physical servers. Hardware based solutions partition an individual server into multiple servers. Regardless of which method is used, end users only see a single server providing access.

When implementing clustered servers, they can be one of the following:

- **Hot:** Indicates that the failover server is up and running with all data and information up-to-date and ready to be used.
- **Warm:** Indicates that the failover server is up and running, but all the data is not up-to-date and requires some type of update to occur to synchronize the data or information.
- **Cold:** Indicates that the failover server is not running, and does not have any data.

Many clustering systems are Hot/Cold; when the production server process (Hot) stops working, the cluster automatically activates the secondary server process (Cold) to take over.

Hot/Cold indicates that when the active server process stops, the other process starts from the ground up, as if you just booted up the computer. For example, if an application server typically takes 20 minutes to start up and become accessible to end users, then the high availability environment must allow for a minimum 20-minute outage for any failure. If the high availability

requirements are for “five-nines,” but the clustering implementation provides a Hot/Cold implementation, then achieving “five-nines” is at risk, because something like a network card failure can be the cause of the (minimum) 20-minute outage.

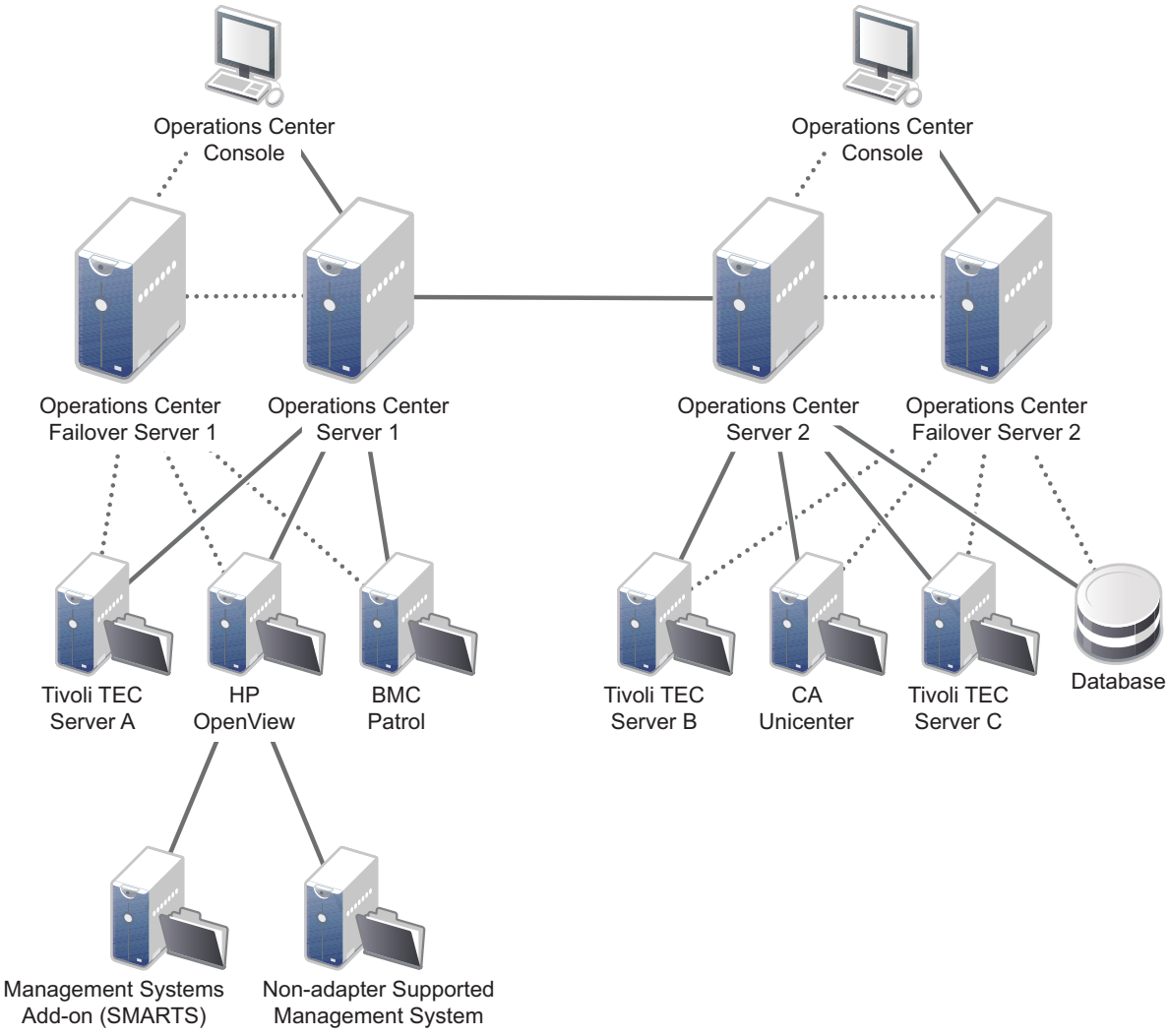
Hot/Warm configurations are faster, but are not transparent to the end users because of the required data synchronization or update time.

Hot/Hot is the best option available, but this option does not guarantee a seamless failover.

6.1.2 Example

Figure 6-1 illustrates a Operations Center implementation that has high availability and fault tolerance.

Figure 6-1 *Operations Center Configuration for High Availability and Fault Tolerance*



Users open a URL to operationscenter.myCompany.com, which sends the user to Operations Center server 1 (left side), or in the event of a failure, users are directed to Failover Operations Center server 1. This achieves the first level of fault tolerance and high availability.

Both Operations Center servers are configured and run at the same time (Hot/Hot) with the same data because of the dual connections to the underlying management systems. The assumption is that the underlying management systems are configured in the same manner.

One Operations Center server can also be configured with dual adapters connected to the primary and backup of each management system.

6.2 Speed

The speed at which users receive data from Operations Center varies depending on such factors as the speed of the LAN/WAN connection, how the management systems are configured in your environment, and the number of adapters and amount of data on your Operations Center server.

To improve speed, you could use a Remote Container server to off-load some adapters from the Operations Center server. You could also use load balancers and redirectors:

- **Load Balancers:** Load balancers are smart technologies that track the amount of resources utilized on an individual server at all times. When new users log in, they are automatically redirected to the server with the lowest utilization rate that can provide the requested service. This common practice distributes end user loads evenly across multiple servers.
- **Redirectors:** Redirectors are sometimes built into load balancers. This type of technology is used as software based clustering (or could be a physical box). Redirectors detect when a service is no longer available on a particular server and redirects existing or new end users to another available server.

6.3 Firewalls

An important configuration consideration is the use of firewalls in your environment. Is there a firewall between the Operations Center server and end users? Is there a firewall between the Operations Center server and the underlying management systems?

A common approach is to place a firewall between the external Internet world and the local network, but allow external users to access the Operations Center server over the Internet. By default, Operations Center is installed with a specific port for HTTP and a range of ports for the IIOP communications. In most cases, you should configure the Operations Center server to utilize one specific port for IIOP, then configure the firewall to allow external traffic to access the internal network using this specific port.

Other variations might require the Operations Center server to connect through a firewall to a data source, such as a management system or a database. In some cases this is an easy exercise. However, depending on the data source, internal security policies might not allow the communication.

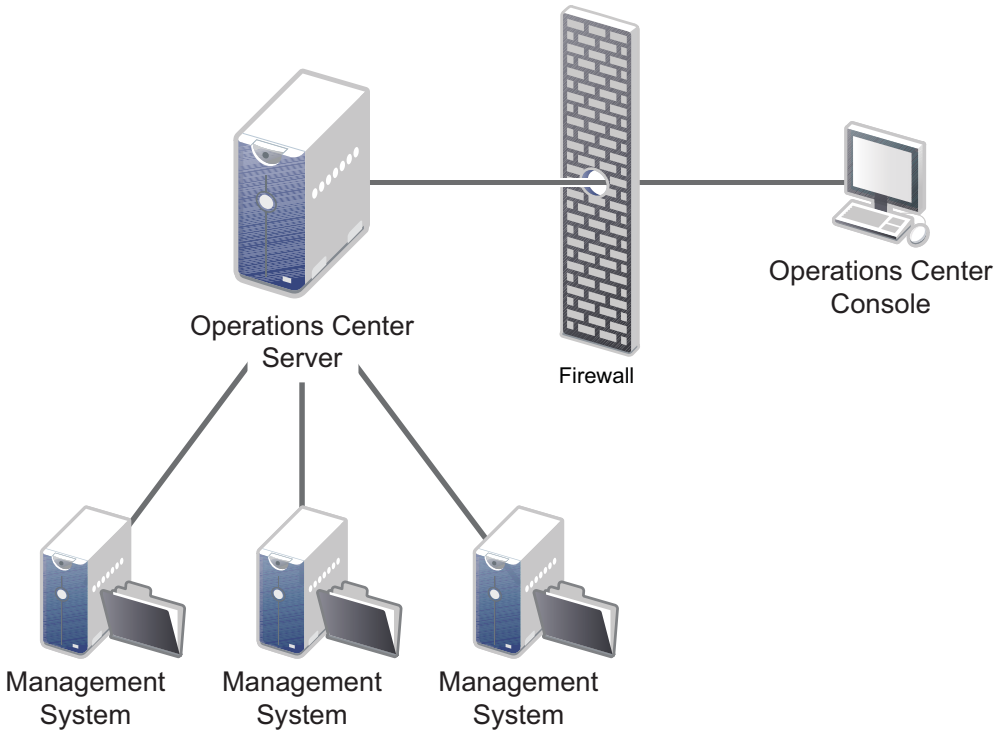
Review the following sections for information on using firewalls:

- Section 6.3.1, “Firewall between Operations Center server and Console,” on page 51
- Section 6.3.2, “Firewall between Operations Center server and Management Systems,” on page 52
- Section 6.3.3, “Operations Center server in DMZ,” on page 53

6.3.1 Firewall between Operations Center server and Console

Figure 6-2 shows a Operations Center system with users who are outside the network:

Figure 6-2 *Operations Center Configuration for Users Outside the Network*

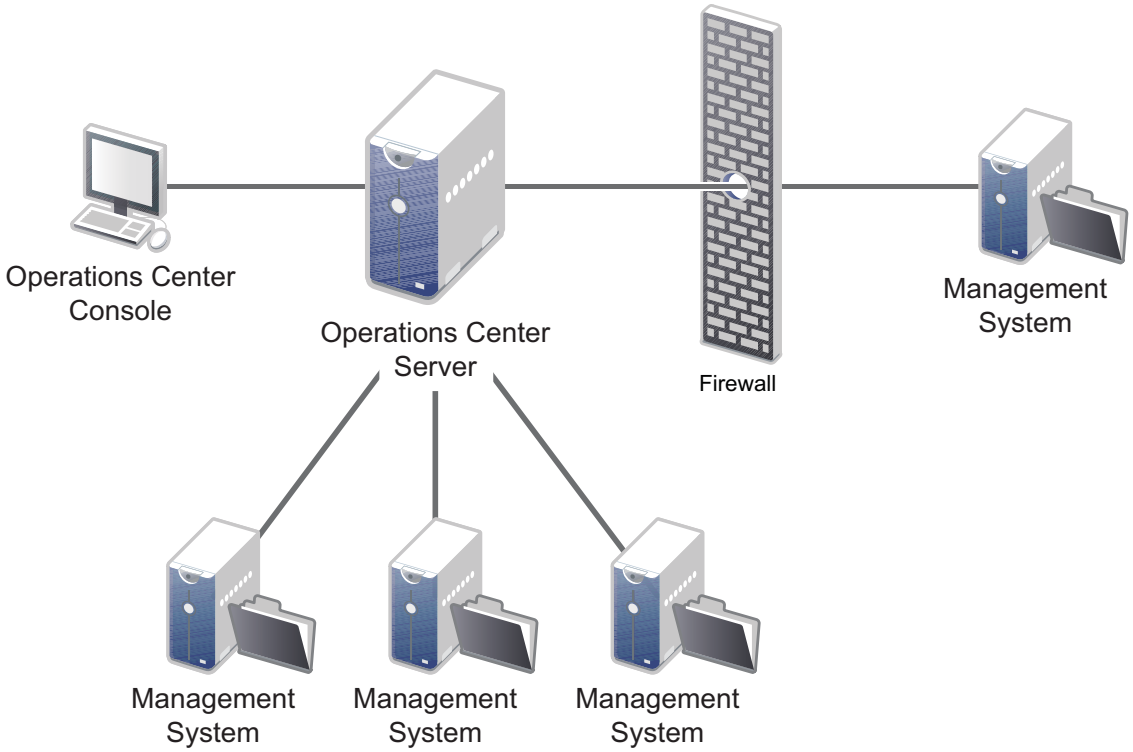


For the dashboard, the only connection established from the outside is the HTTP or HTTPS port specified. Operations Center consoles require the HTTP or HTTPS and the IIOP (Corba) port.

6.3.2 Firewall between Operations Center server and Management Systems

Figure 6-3 shows a firewall between the Operations Center server and an actual data integration point, such as an IBM Micromuse Netcool system, a database through BDI, or an HP OpenView NNM:

Figure 6-3 *Firewall Configuration between Operations Center server and Management Systems*



Each system allows a ports to be configured on the firewall to enable communication. The specific port could be a configurable item on the adapter, ORB, or in the underlying management system.

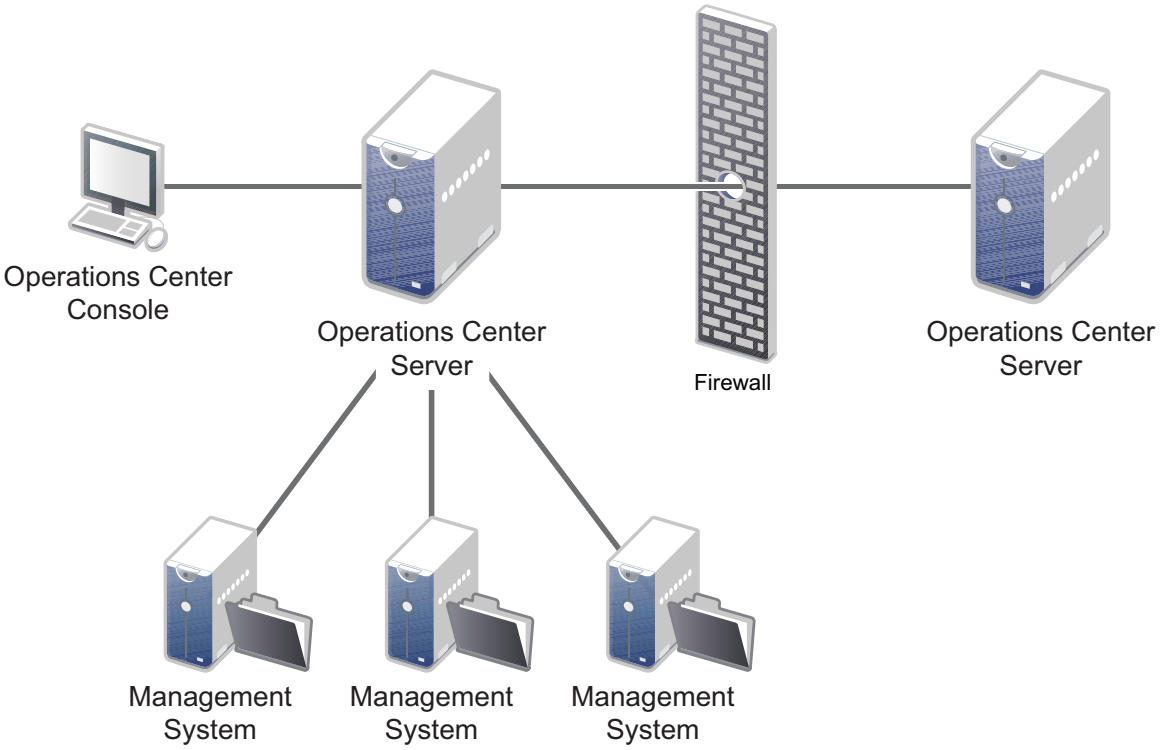
For example, for Netcool, configure the port in the Netcool system. The Operations Center adapter is informed of the port to use. In the case of OpenView, during the ORB installation, use the option to specify the port. Then specify the same port number in the OpenView adapter properties.

6.3.3 Operations Center server in DMZ

In computer security, a demilitarized zone (DMZ), more appropriately known as demarcation zone or perimeter network, is a physical or logical subnetwork that contains an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN).

Figure 6-4 shows an example of a Operations Center system outside the network in a DMZ:

Figure 6-4 *DMZ Configuration for Operations Center*



The Operations Center system on the outside is configured with an ICA adapter. The DMZ server can have views for the Operations Center console and/or the dashboard. Regardless, the firewall traversal requires the initial HTTP or HTTPS connection as well as the IIOP connection.

7 Production Environment Configurations

Before deploying any new system in your environment, you should test it in a development environment. After you have tested Operations Center in a development environment and have it set up as you want it, you should replicate that same set up in your actual environment, or production, environment. You can do this through actions taken on the Operations Center configuration:

7.1 About Configurations

A configuration for the Operations Center server is defined as the hierarchy of elements in the Operations Center server as well as relationships between the objects, data collection settings, and other setting and parameter information.

Each Operations Center server can run one configuration at a time. You can have multiple configurations set up to run at different times for different uses.

The following actions can be taken with Operations Center server configurations:

- Create
- Modify
- Copy
- Delete
- Share
- Move (import/export)

Configurations are stored in the Configuration Storage data source and can be copied from one database to another.

7.2 Copying Configurations

A Operations Center configuration might need to be copied from one machine (source) to another (target) machine for various reasons including:

- Promoting a test server configuration to a production server.
- Two identical Operations Center servers are configured for fault tolerance (high availability) purposes.
- A backup copy of customizations to the Operations Center configuration needs to be created without retaining the entire directory structure.
- Migrating configuration settings from the default database to an external database.

You can copy an entire configuration and move it from one server to another. You can then rename configuration files and easily switch between configurations by renaming and restarting the server.

You can also import and export configurations or portions of a configuration from one Operations Center server to another. For example, you can export just a portion of the elements in the hierarchy as displayed in the Operations Center console. For more information, see the *Operations Center 5.5 Server Configuration Guide*.