VMware Smart Assurance Service Assurance Manager Introduction

VMware Smart Assurance 10.0.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 Preface 4

- Purpose 4
- Audience 5
- VMware Smart Assurance Service Assurance Manager installation directory 5
- VMware Smart Assurance Service Assurance Manager 5
- Related documentation 6
- VMware Smart Assurance Service Assurance Manager documentation 6
- Conventions used in this document 7
- Where to get help 8
- Your comments 9

2 Architectural Overview 10

- Service Assurance Manager architecture 10
- Service Assurance modules 14

3 Functional Overview 17

- Service Assurance Manager features and functions 17
- Automatic topology and event consolidation 17
- Automatic topology abstraction 18
- Global Console 18
- Service Assurance functions 21
- Service Assurance module functions 25

4 Implementation Scenarios 28

- Challenges of network management 28
- VMware Smart Assurance solutions 28
- Enterprise provider 30
- Network service provider 32

Preface

1

As part of an effort to improve its product lines, VMware periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your VMware representative if a product does not function properly or does not function as described in this document.

Note This document was accurate at publication time. New versions of this document might be released on the VMware online support website. Check the VMware online support website to ensure that you are using the latest version of this document.

This chapter includes the following topics:

- Purpose
- Audience
- VMware Smart Assurance Service Assurance Manager installation directory
- VMware Smart Assurance Service Assurance Manager
- Related documentation
- VMware Smart Assurance Service Assurance Manager documentation
- Conventions used in this document
- Where to get help
- Your comments

Purpose

The Service Assurance Manager (Service Assurance) solution automatically correlates topology and event data from multiple VMware Smart Assurance managed domains to diagnose root-cause problems and (with Business Impact Manager) the impact that those problems have on business-critical processes and services. VMware Smart Assurance managed domains can include IP networks, systems, routing protocols, ATM/Frame Relay, applications, and business entities. Service Assurance Manager enables operations personnel to effectively prioritize their time and resources to maintain and sustain the business-critical processes and services.

VMware Smart Assurance Service Assurance Manager Introduction provides high-level architectural and functional overviews of the VMware Smart Assurance Service Assurance Manager solution. It also provides several examples of implementation scenarios.

Audience

This document is intended for operations staff, managers, and administrators who are interested in automated Service Assurance solutions.

VMware Smart Assurance Service Assurance Manager installation directory

In this document, the term BASEDIR represents the location where VMware Smart Assurance software is installed:

- For UNIX, this location is: /opt/InCharge/<*productsuite*>.

  For example, on UNIX operating systems, VMware Smart Assurance Service Assurance Manager is, by default, installed to /opt/InCharge/SAM/smarts.

  Optionally, you can specify the root of BASEDIR to be something other than/opt/InCharge (on UNIX), but you cannot change the <*product*> location under the root directory.

  The VMware Smart Assurance System Administration Guide provides more information about the directory structure of VMware Smart Assurance software.

VMware Smart Assurance Service Assurance Manager

The VMware Smart Assurance Service Assurance Manager includes the following products:

- Service Assurance Manager (Global Manager), includes Business Impact Manager (BIM) and Failover System
- Global Console
- Business Dashboard
- Companion UI
- SAM Native Adapters:
  - Service Assurance Manager Notification Adapters (E-Mail Notifier Adapter, Script Notifier Adapter, SNMP Trap Notifier Adapter, Log File Notifier Adapter)
  - Adapter Platform (Adapter Platform server, Syslog Adapter, SNMP Trap Adapter, sm_ems command-line interface)
  - XML Adapter
  - VMware Smart Assurance Adapter for UIM/O

Related documentation

In addition to this document, VMware Corporation provides a help system for command line programs as well as product documentation.

Help for command line programs

Descriptions of command line programs are available as HTML pages. The index.html file, which provides an index to the various commands, is located in the BASEDIR/smarts/doc/html/usage directory.

VMware Smart Assurance documentation

Readers of this guide may find the following related documentation helpful:

- Smarts Foundation EMC Data Access API (EDAA) Programmer Guide
- VMware Smart Assurance Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products
- VMware Smart Assurance Common Information Model (ICIM) Reference for Service Assurance Manager
- *VMware Smart Assurance Foundation Documentation Portfolio*
- VMware Smart Assurance System Administration Guide
- VMware Smart Assurance ASL Reference Guide
- VMware Smart Assurance Perl Reference Guide
- VMware Smart Assurance Dynamic Modeling Tutorial
- VMware Smart Assurance MODEL Reference Guide

Note These documents are updated periodically. Electronic versions of the updated manuals are available on the VMware online support website:

docs.vmware.com

VMware Smart Assurance Service Assurance Manager documentation

The following documents are relevant to users of the VMware Smart Assurance Service Assurance Manager:

- VMware Smart Assurance Service Assurance Manager Release Notes
- VMware Smart Assurance Open Source License and Copyright Information
- VMware Smart Assurance Service Assurance Manager Introduction
- VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers

- VMware Smart Assurance Service Assurance Manager Deployment Guide
- VMware Smart Assurance Service Assurance Manager Configuration Guide
- VMware Smart Assurance Service Assurance Manager Operator Guide
- VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide
- VMware Smart Assurance Business Impact Manager User Guide
- VMware Smart Assurance Failover System User Guide
- VMware Smart Assurance Service Assurance Manager Notification Adapters User Guide
- VMware Smart Assurance Service Assurance Manager Adapter Platform User Guide
- VMware Smart Assurance Adapter for Unified Infrastructure Manager/Operations Configuration Guide
- VMware Smart Assurance XML Adapter User Guide
- VMware Smart Assurance Notification Module User Guide
- VMware Smart Assurance Service Assurance Manager Troubleshooting Guide
- VMware Smart Assurance Companion UI Online Help
- VMware Smart Assurance Companion UI Open Source License and Copyright Information for GPLv3 as Included with a Distribution of SLES 11
- VMware Smart Assurance Service Assurance Manager Documentation Portfolio

  The VMware Smart Assurance Documentation Catalog provides documentation resources for other VMware Smart Assurance products.

Conventions used in this document

VMware uses the following conventions for special notices:

Note NOTICE is used to address practices not related to personal injury.

Typographical conventions

VMware uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: ■ Names of interface elements ■ Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities ■ URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages

	Used in procedures for: ■ Names of interface elements ■ What the user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: ■ Full titles of publications referenced in text ■ Emphasis, for example, a new term ■ Variables
`Courier`	Used for: ■ System output, such as an error message or script ■ URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: ■ Variables on the command line ■ User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Pathname conventions

Directory pathnames are shown with forward slashes (/).

Graphical conventions

Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser, an open circle appears for UNIX.

Manager

Unless otherwise specified, the term Manager is used to refer to VMware Smart Assurance programs such as Domain Managers, Global Managers, and adapters.

Where to get help

VMware support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware products, licensing, and service, go to the VMware online support website (registration required) at:

```
docs.vmware.com
```

For technical support, Create Service Requests or Contact Customer Service on VMware Online Support at support.vmware.com. To open a service request through VMware Online Support, you must have a valid support agreement. Contact your VMware Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Provide your feedback of this document to:docs.vmware.com.

Architectural Overview

2

This chapter provides an architectural overview of
VMware Smart Assurance Service Assurance Manager(Service Assurance), the
Service Assurance Manageradapters, and the Service Assurancemodules
(VMware Smart Assurance Business Impact Manager, Global Console, and Business Dashboard) that can be implemented to extend the capabilities of Service Assurance.

VMware Smart Assurance Service Assurance Manageris a solution for managing the technology infrastructure that supports business services. As the cornerstone of network operations management, it provides integrated, unified, and individualized views of the systems, network infrastructure, applications, and business entities that comprise the managed domain.

Service Assurance Managerimports topology and event information from the underlying managed domains (distributed management applications), consolidates the information, and interprets problems in the context of their impact on business services. Service Assuranceprovides operations personnel with meaningful information with which automated corrective actions can be associated.

The Service Assurancemodules provide the capabilities to calculate the business impact of infrastructure problems, to produce a wide variety of operational and management reports, and to display customer-specific information to a given enterprise or service provider customer through a secure channel.

This chapter contains the following information:

- Service Assurance Manager architecture
- Service Assurance modules

This chapter includes the following topics:

- Service Assurance Manager architecture
- Service Assurance modules

Service Assurance Manager architecture

VMware Smart Assurance Service Assurance Manager architecture illustrates the
VMware Smart Assurance Service Assurance Manager architecture.

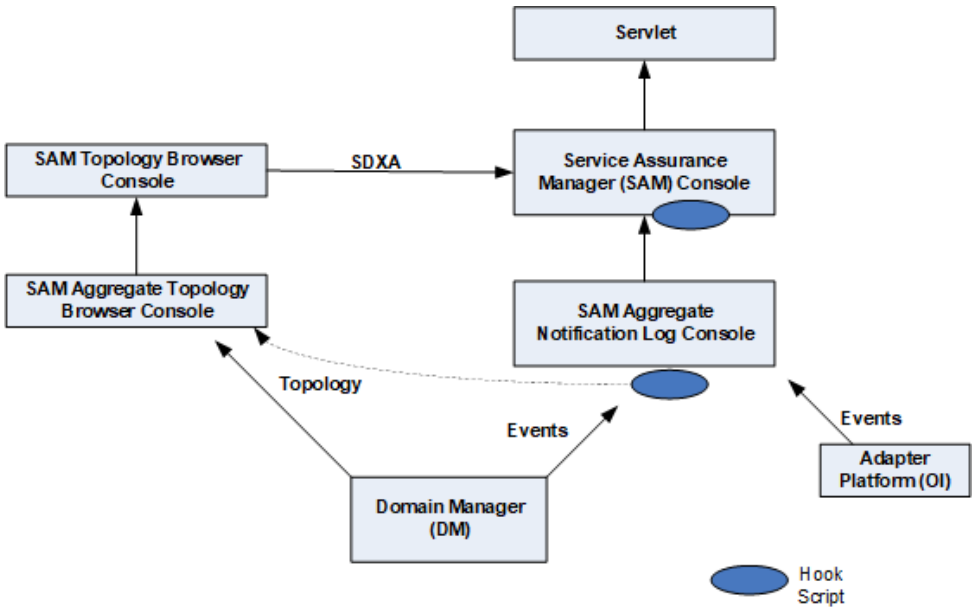


Figure 2-1. VMware Smart Assurance Service Assurance Manager architecture

VMware Smart Assurance Service Assurance Manager abstracts topology information and cross-correlates and consolidates event information from distributed VMware Smart Assurance applications and third-party applications.

Note VMware Smart Assurance applications are responsible for discovering and monitoring infrastructure elements, and correlating event information within their respective managed domains.

Service Assurance Manager, other VMware Smart Assurance applications, or third-party applications communicate by way of a shared Information Bus that employs the VMware Smart Assurance Common Information Model™ (ICIM). After Service Assurance abstracts high-level views of the distributed topologies from the underlying applications, it correlates, consolidates, and integrates event information collected from the applications, and enriches the event information with the severity of the events.

Event information (for example, root-cause problems and their impacts and severities) are displayed in the Notification Log Console, Topology Browser Console, Map Console, or Summary View Console. From these consoles, operations personnel can invoke diagnostic or corrective tools, store the information for management and operations reports, and send the information to third-party applications.

Service Assurance Manager

The Service Assurance Manager, also referred to as the Global Manager, is the Service Assurance component that serves as the central point for monitoring and managing your entire technology infrastructure by obtaining data from multiple distributed domains. The Global Manager communicates with the underlying distributed VMware Smart Assurance applications and abstracts and consolidates:

- Network, system, application, and business resources
- Results of domain-specific root-cause analysis

- Results of domain-specific impact analysis

  The Global Manager scales to large topologies because it maintains a high-level, abstract representation of the topology. The detailed topology information — and therefore the bulk of the data — is kept in other VMware Smart Assurance applications. When needed, the Global Manager retrieves detailed information from the underlying domains.

  The Global Manager can attach to multiple, distributed VMware Smart Assurance applications as well as other Global Managers. It can also be integrated with third-party applications from which it can receive topology and event information, and to which it can send event information or initiate corrective actions.

  The Global Manager, in conjunction with Report Manager, sorts and stores event-related information in an ODBC-compliant database from which users can produce a variety of management, operations, and business impact reports.

Global Console

VMware Smart Assurance Service Assurance Manager includes a user interface that provides different views into VMware Smart Assurance-managed domains.

The Global Console displays topology and notifications as well as summary, containment, and status information. VMware Smart Assurance operators use the Global Console to monitor VMware Smart Assurance domains, acquire detailed information (on demand) about topology and events, respond to problems, and take corrective action. VMware Smart Assurance administrators with appropriate privileges and access control can use the Global Console to discover topology, and administer underlying domains, as well as administer VMware Smart Assurance users, user profiles, program tools, and escalation policies.

The Global Console runs as a standalone Java program.

Companion User Interface

VMware Smart Assurance Service Assurance Manager Companion User Interface (SAM Companion UI) supplements existing functionality in SAM, VMware Smart Assurance Network Configuration Manager (NCM) and Watch4net Automated Performance Grapher (APG).

The SAM Companion UI is a VMware®-based appliance, that is, a virtual machine. The VMware Smart Assurance SolutionPack Installation and Configuration Guide provides detailed information about installing and configuring the SAM Companion UI.

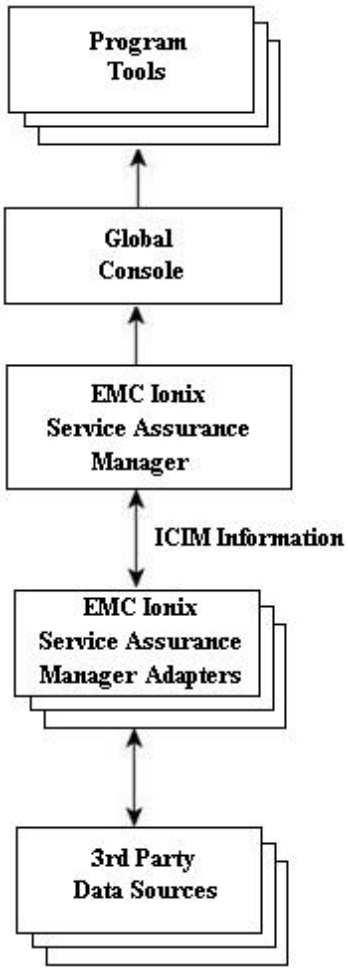
Integration with third-party applications

Because VMware Smart Assurance Service Assurance Manager is an open solution, it is possible to integrate Service Assurance with third-party applications and other VMware Smart Assurance applications by way of Service Assurance Manager (SAM) adapters, as shown in Integration with third-party applications.

The VMware Smart Assurance Service Assurance Manager Adapter Platform, which normalizes data in accordance with the ICIM, enables the import or export of topology and event information. The topology information is stored in the repository of the Global Manager. As event data is forwarded to Service Assurance through the adapters, the system correlates the third-party event data with the corresponding elements in the Global Manager's repository.

SAM adapters also enable VMware Smart Assurance Service Assurance Manager to forward event information to third-party applications, such as trouble ticketing systems.

Figure 2-2. Integration with third-party applications



VMware Smart Assurance Adapter for UIM/O

The VMware Smart Assurance Adapter for Unified Infrastructure Manager/Operations (referred to as the VMware Smart Assurance Adapter for UIM/O) provides integration between the VMware Smart Assurance Adapter for Unified Infrastructure Manager/Operations (here in referred to as UIM/O) and the Service Assurance Manager. The adapter retrieves alerts from UIM/O, creates notifications from the alerts, and sends the notifications to the Global Manager.

The
VMware Smart Assurance Adapter for Unified Infrastructure Manager/Operations Configuration Guide provides deployment information, configuration instructions, and client tool examples.

Service Assurance Failover System

To maintain critical availability, VMware Smart Assurance Service Assurance Manager can be implemented with a failover system. The
VMware Smart Assurance Service Assurance Manager Failover System ensures that the managed environment continues to be monitored when the primary Global Manager becomes unavailable because of a hardware failure or system malfunction. Redundancy is provided by a secondary Global Manager that serves as a backup to the primary Global Manager. The Failover System, which is configured to match the primary system, monitors the primary Global Manager. The Failover System periodically copies the repository file to the secondary Global Manager, thus preserving important topology and configuration information.

If a failure occurs, the secondary Global Manager automatically starts. The secondary Global Manager registers with the VMware Smart Assurance Broker using the name of the primary Global Manager. Clients of the primary Global Manager (such as the Global Console and adapters) that become disconnected can reconnect to the secondary Global Manager.

When the primary Global Manager is again available to monitor the managed environment, a reset script copies the backup repository to the primary Global Manager, shuts down the secondary Global Manager, and restarts the primary Global Manager.

Service Assurance modules

Several modules can be implemented with VMware Smart Assurance Service Assurance Manager to extend Service Assurance's capabilities. These include:

- VMware Smart Assurance Business Impact Manager.
- VMware Smart Assurance Report Manager.
- VMware Smart Assurance Web Console.
- VMware Smart Assurance Business Dashboard.

VMware Smart Assurance Business Impact Manager

VMware Smart Assurance Business Impact Manager (Business Impact Manager) extends the capabilities of Service Assurance to analyze events by calculating the business impact of events and propagating the impacts to affected business entities as discrete notifications that are linked to topology within the managed domain. The impacts are displayed in the Business Services Maps.

To accomplish its functions, Business Impact Manager includes facilities to import business entities, which consist of subscribers and service offerings. Subscriber information may include customers as well as organizations, business units, lines of business, and department entities. Service offerings include business processes. For example, a subscriber can be a customer that subscribes to an IT service offering that provides Internet access.

The imported business information can be also assigned to user-specified groups.

Additionally, Business Impact Manager provides facilities to assign weights to business entities and other elements in your topology. The weights capability allows you to prioritize critical topology and to use the prioritized information when calculating the business impact of events.

VMware Smart Assurance Report Manager

VMware Smart Assurance Report Manager (Report Manager), which includes a Structured Query Language (SQL) Data Interface, extracts notifications from Service Assurance, passes them to an Open Database Connectivity (ODBC) driver, and stores the notification information in a relational database. The database uses a special database schema designed for VMware Smart Assurance notifications.

Notification information can then be extracted from the database and imported into Crystal Enterprise Reports or some other user-selected report application.

The Report Manager includes predefined report files (in Crystal format) that can be used to display or print a wide variety of operational, management, and business impact reports.

VMware Smart Assurance Web Console

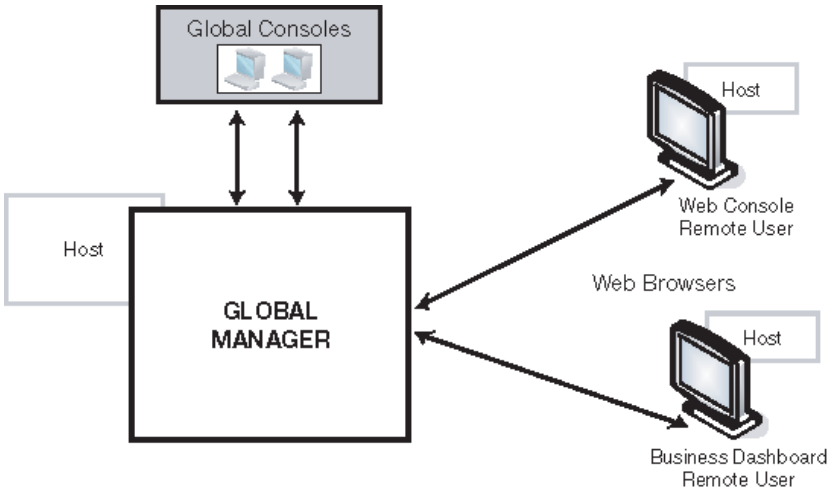
The contents of the Global Console can also be displayed as a Java applet within a web browser. The Web Console capability allows you to connect to a Domain Manager from any system with a web browser and does not require a Global Console installation on the system.

VMware Smart Assurance Business Dashboard

The VMware Smart Assurance Business Dashboard (Business Dashboard) is a flexible, business-oriented alternative to the Web Console. The Business Dashboard displays a collection of VMware Smart Assurance analysis data alongside important data from other sources. Components of the collection of VMware Smart Assurance data are referred to as VMware Smart Assurance ViewletsTM. The collection of viewlets can be loaded into your organization's web page and can commingle with important trouble-ticketing information or your company's intranet news. VMware Smart Assurance viewlets can also be embedded within a third-party Web Portal product.

Web Console and VMware Smart Assurance Business Dashboard architecture illustrates the architecture of a Web Console and an VMware Smart Assurance Business Dashboard when loaded by a remote user.

Figure 2-3. Web Console and VMware Smart Assurance Business Dashboard architecture



Functional Overview

3

This chapter includes the following topics:

- Service Assurance Manager features and functions
- Automatic topology and event consolidation
- Automatic topology abstraction
- Global Console
- Service Assurance functions
- Service Assurance module functions

Service Assurance Manager features and functions

Service Assurance Manager provides the automated functions and features that are required by today's enterprise and service provider network operations centers. Its automation, intelligent analyses, and adaptability can significantly reduce both the resources needed for pinpointing and resolving infrastructure problems, and the costs of monitoring and managing distributed networks.

Automatic topology and event consolidation

One of the primary tasks of VMware Smart Assurance Service Assurance Manager is topology and event consolidation. Service Assurance Manager imports infrastructure elements (such as hosts and routers) and applications from each underlying managed domain. As it imports the elements, it consolidates elements that are reported by different sources. Service Assurance Manager also imports the relationships between the elements from the underlying managed domains. Using these relationships and overlapping devices, Service Assurance Manager accurately pieces together a complete topology of the managed environment.

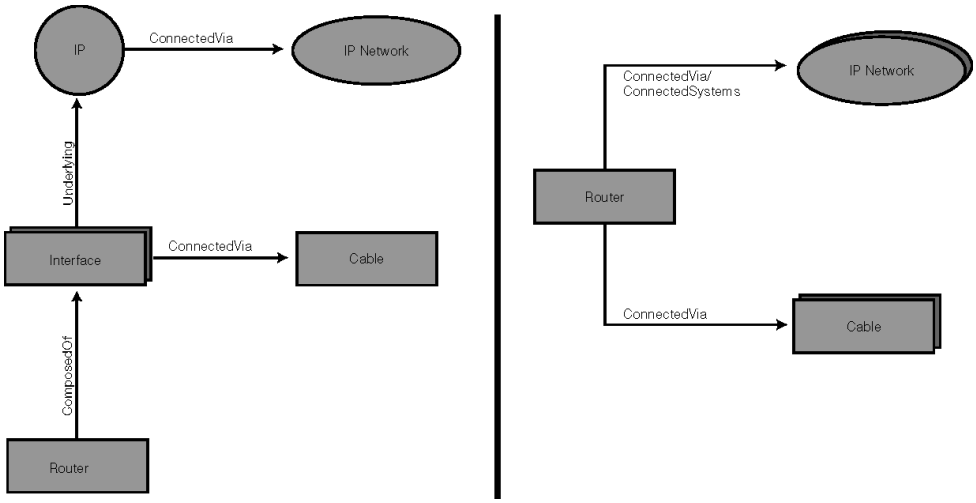
When Service Assurance Manager imports events from the underlying managed domain, they are automatically associated with the elements to which they apply. Notifications received from multiple sources are consolidated into single events. Similarly, impacts reported by different sources for the same problem are deduplicated and associated with the consolidated event in Service Assurance Manager.

Further, to provide business context, VMware Smart Assurance Service Assurance Manager provides a facility that imports customer and service information from provisioning systems and other sources. Using this data, Service Assurance Manager can automatically calculate the customer and service impact for the consolidated events.

Automatic topology abstraction

In order to scale to large numbers of underlying systems, VMware Smart Assurance Service Assurance Manager performs topology abstraction. Difference between detailed and abstracted representation illustrates the difference between a detailed representation and an abstracted representation of network connectivity.

Figure 3-1. Difference between detailed and abstracted representation



Abstraction produces a coarse level of topology detail. A system, for example, is viewed as a single entity rather than as a collection of its components, and connectivity is between systems as opposed to between components in the system.

Although Service Assurance maintains a coarse level of topology detail, it stores sufficient information for its varied Notification Log, Topology Browser, and Map views. When needed, detailed information can be automatically retrieved from the underlying applications by Service Assurance.

Global Console

The Global Console provides a focal point through which operations personnel can monitor and manage distributed systems and VMware Smart Assurance administrators can configure and administer Domain Managers. VMware Smart Assurance administrators control the views, program tools, and access to console operations for VMware Smart Assurance users. The following describes the full functionality of each console. Certain functions require a license and thus may not be included in your VMware Smart Assurance deployment. Also, an VMware Smart Assurance user's access to some console operations may be restricted based on the user's connection privileges and user profile.

For any given event, operations personnel with appropriate access control can take ownership of the event, acknowledge the event, add comments to the audit log of the event, or invoke tools for corrective actions.

The Global Console provides the following console views:

- Notification Log Console

- Topology Browser Console
- Map Console
- Summary View Console
- Status Table Console
- Domain Manager Administration Console
- Global Manager Administration Console

Notification Log Console

The Notification Log Console provides a view of a set of notifications, which is defined by the user profile associated with the user. The notification information can include, for example, the type of event, the element that is affected, and the severity of the event. Operations personnel can potentially open multiple Notification Log Consoles, each customized to display different events, or show multiple lists in a single console, as needed.

Operations personnel can also potentially access the details of the event through the use of the Notification Properties dialog box. The Notification Properties dialog box provides detailed information about a selected notification. The properties include, for example, attributes and values related to this event, elements that are impacted by this event, an audit log of changes in this event's history, or (if this event is a root-cause problem) other events used in the analysis.

The viewable attributes of the displayed events in the Notification Log view (for example, event severity, active event, or first notify) can be customized to meet the needs or preferences of operations personnel. The order in which the attributes are displayed can also be modified. Operations personnel can sort on any number of attributes (whether the attribute column is visible or not) by specifying up to five sorting columns.

The notifications listed in the Notification Log view are color-coded in accordance with the severity of the events. An icon is also used as another indicator of an event's severity.

Topology Browser Console

The Topology Browser Console enables operations personnel to display the managed topology in a tree format and traverse the topology. The console displays Domain Managers as well as Global Managers. For the selected managed domain, the console displays the classes of elements, instances of each class, and their relationships. Specified elements, a circle (on UNIX systems), can be expanded into instances, properties, or relationships.

When an element in the topology tree is selected, the console displays a corresponding property sheet with tabs for Attributes, Events, and Groups. The tabs, where applicable, include the following information:

- Attributes — Provides general information about the selected element
- Events — For a selected Global Manager, displays the active events that Service Assurance may notify for the element

- Groups — Provides the current group membership of the element

  In addition, the Topology Browser Console provides the Browse Detail menu option. When an element in the topology tree is selected, Browse Detail displays a list of all underlying managed domains that contain that element in their topology. Users can select an underlying managed domain and display it in another Topology Browser view. For hierarchical Service Assurance deployments, users can select Browse Detail as many times as necessary to navigate to the desired domain. Note that Browse Detail is also available for selected notifications in the Notification Log Console and for selected map icons and edges in the Map Console.

Map Console

The Map Console displays, by way of icons and edges, the managed elements in a given environment and the relationships between them. Different types of maps are made available based upon the elements in your managed topology. For example, with
VMware Smart Assurance IP Availability Manager, the console displays infrastructure elements in network and connectivity maps. With the addition of Business Impact Manager, the console can also display business services maps that show how the infrastructure elements are associated with business services, as well as the customers that subscribe to those services.

Operations personnel can select elements in the maps and then display detailed information about the elements, such as the ports or interfaces contained in a system.

If the status of a given element displayed in the Map Console indicates a problem, operations personnel can view the audit logs of events by way of the Notification Properties dialog box. They can also select and use tools such as on-demand pings and Telnet sessions.

The maps can be customized to meet your needs or preferences. For example, custom backgrounds and element icons can be incorporated into the maps.

Summary View Console

The Summary View Console provides overviews or summaries of notifications. The console can contain several summaries that are attached to either the same managed domain or to different domains.

Summaries offer concise, graphical representations of sets of notifications associated with groups of elements. The summary can be depicted as a three-dimensional graph or pie chart. The summary counts indicate the percentages of elements in the group with active events.

The summaries organized by severity are color-coded in accordance with the severity of the events. Otherwise, for other criteria, the colors do not indicate event status.

Status Table Console

A Business Impact Manager user can view a Status Table to quickly determine the overall status of customers and the services being delivered to those customers. In such a Status Table, customers would be represented as the primary set of instances, and the services being delivered to them would be represented as the secondary set of instances.

To describe it in more general terms, a Status Table Console offers another way to present a concise status of a set of instances. The information appears as a matrix, with a primary set of instances along the y-axis and a secondary (related) set of instances along the x-axis. The status of the related instances appears, when relevant, at the intersection points in the matrix to reflect the overall status for each primary instance.

The Status Table functionality is very useful for the Business Impact Manager user. The Status Table requires a Web Console or VMware Smart Assurance Business Dashboard license.

Domain Manager Administration Console

The Domain Manager Administration Console enables VMware Smart Assurance administrators to configure and administer the underlying Domain Managers, and to perform tasks such as:

- Discover topology
- Manage and unmanage elements in the managed topology
- Access the Polling and Thresholds Console to fine-tune parameters of the polling and thresholds settings in the underlying domain

  The VMware Smart Assurance Storage Insight Management Suite Discovery Guide provides information about the Domain Manager Administration Console. Information about polling and thresholds for specific VMware Smart Assurance applications is provided in their respective user guides.

Global Manager Administration Console

The Global Manager Administration Console enables VMware Smart Assurance administrators to configure Global Managers, including Security Infrastructure Managers (SIMs), and the SAM Adapter Platform.

For a selected Global Manager, VMware Smart Assurance administrators create and maintain configuration entities such as notification lists, tools, users, user profiles, access control to console operations, and escalation policies.

The VMware Smart Assurance Service Assurance Manager Configuration Guide contains information about the Global Manager Administration Console.

Service Assurance functions

The following section describes many of the functions that are integral to the VMware Smart Assurance Service Assurance Manager.

Notification severity

The VMware Smart Assurance Service Assurance Manager classifies notifications according to their calculated severity.

The notifications listed in the Notification Log Console and the Map Console are color-coded in accordance with the severity of the events. Icons are also used in the notification log and the maps to identify severity.

The color codes are explained in Notification severity levels.

Table 3-1. Notification severity levels

Level	Icon	Color	Description
1		Red	Critical — Identifies a specific failure that requires resolution.
2		Orange	Major — Identifies a serious condition that requires immediate attention.
3		Yellow	Minor — Identifies an abnormal condition that is not serious but requires some action.
4		Blue	Unknown — Identifies an unknown, unreachable, disconnected, or suspended condition.
5		Green	Normal — The element is in its normal state.

Notification List

A Notification List determines the events that are forwarded to a given client. Essentially, the list filters the notifications that are sent from the Global Manager to a client. Additionally, the list, which is configured by the VMware Smart Assurance administrator, can be assigned to one or more user profiles. The personnel assigned to a specified list only see the set of events defined by the list.

The lists could be used to organize, for example:

- Business units
- Geographical regions
- Groups of resources

  During day-to-day operations, operations personnel use the Global Console to monitor and manage their areas of responsibility. In doing so, personnel see only the subset of notifications defined for them in the Notification List.

  VMware Smart Assurance adapters can also connect to a Notification List, and receive the notifications that match the conditions specified in the list.

  The VMware Smart Assurance Service Assurance Manager Configuration Guide contains information about Notification Lists.

Tools

Tools are programs that are executed by VMware Smart Assurance Service Assurance Manager. There are two types of tools:

- Server and client tools can be invoked by operations personnel in the Global Console or can be automated using escalation policies. Tools invoked by operators may produce output that can be sent back to the console for display.
- Automatic tools are executed by administrator-specified escalation policies or by adapters. Output is not sent back to the console for display.

  Server and client tools are executed in the context of a particular target object. The target object may be a notification, or it may be an infrastructure element such as a router. When invoked from the Global Console, the specification of the target object is implicit.

  Automatic tools are executed for notifications that meet the escalation criteria for specified periods of time.

  The VMware Smart Assurance Service Assurance Manager Configuration Guide contains additional information about the Service Assurance tools.

Notification escalation

Escalation is a process that defines a sequence of corrective actions for notifications. Examples of corrective actions include alerting responsible parties and executing automatic tools.
VMware Smart Assurance administrators use the Escalation view in the Global Manager Administration Console to configure escalation policies.

Escalation policies enable VMware Smart Assurance administrators to automate responses to events. For example, an administrator can configure an escalation policy to page a shift supervisor if no one takes ownership of a problem for more than 15 minutes. If the problem remains unowned for 30 minutes, the policy will page the operations manager. The administrator can define multiple policies to handle different types of events.

Audit log

An audit log is associated with each of the notifications that the
VMware Smart Assurance Service Assurance Manager receives from the underlying
VMware Smart Assurance applications. The audit log includes the following information:

- Event
- Time of the update
- Name of the operations person or system that made the update
- Type of audit entry

- Description of the entry (for example, Notify, Clear, or Suspend)

  Service Assurance begins to create an audit log when it receives a notification, and relates the event to an infrastructure element. Thereafter, Service Assurance adds actions for the event, any program tools used for the event, and changes in the status of the event. Actions may include system actions such as archiving and user actions such as acknowledgement and ownership. Comments can be added directly to the audit log.

  An audit log for each notification can be viewed in an audit log dialog box using the Global Console, exported to spreadsheet applications, or printed as part of a report. All the audit log entries for individual notifications are stored in one log file on the Global Manager.

Containment

The Containment dialog box provides detailed information about a managed element. Containment information varies depending upon the type of element and the type of analysis being performed by the underlying domain. As examples, for a network connection, the containment information includes details about connection points; for a device managed by IP Performance Manager, containment information includes details about the device's memory.

The Containment dialog box is available for selected notifications in the Notification Log Console, for selected instances in the Topology Browser Console, and for selected nodes in the Map Console. When an element is managed by multiple Domain Managers, the Containment dialog box includes all the containment information for each domain.

Security

Security is a critical concern in the world of large-scale distributed networks. Therefore, the VMware Smart Assurance Service Assurance Manager provides several means by which VMware Smart Assurance administrators can set up security and control access to the system. This includes:

- User rights and privileges, including client authentication
- Encryption of passwords in files
- Encryption of communication channels
- Support for FIPS 140-2

  An VMware Smart Assurance administrator can place access restrictions on certain console operations by applying user profiles. Each user should be associated with a profile that defines the appropriate level of access control (rights and privileges) for their position and job responsibilities.

  Client/server connections are controlled on both the client and server sides of the system. The system is secured using authentication records and by assigning connection privileges on the server side. When a client initiates a connection to a server, the client must supply appropriate authentication to the server before the connection (as defined by the connection privileges) is permitted.

  For added protection, authentication and other passwords are encrypted in the files that store them.

Communication channels (that is, TCP connections made through Remote API) between VMware Smart Assurance servers, brokers, and adapters can also be encrypted. Instead of passing information as clear text, these components' communications can be encrypted using either a site secret, the Diffie Helman-Advanced Encryption Standard (DH-AES), or both. For new installations, encryption by DH-AES is enabled by default between VMware Smart Assurance processes that support encryption.

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard governing cryptographic modules. FIPS 140 is required for any software purchased by the U.S government and U.S military. This release specifically addresses U.S Government accounts which require FIPS 140 compliance.

A configuration parameter, *SM_FIPS140*, has been introduced for FIPS 140 in the runcmd_env.sh file. The SAM administrator can enable or disable this parameter as required. The default value of this parameter is *FALSE*.

The VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers provides additional information on FIPS 140-2.

The VMware Smart Assurance System Administration Guide contains additional information about securing access to VMware Smart Assurance applications. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes additional information about restricting access to certain Global Console operations.

Service Assurance module functions

The Service Assurance modules provide additional capabilities to calculate the business impact of infrastructure problems, to produce a wide variety of operational and management reports, and to display customer-specific information to a given enterprise or service-provider customer through VMware Smart Assurance Business Dashboard.

VMware Smart Assurance Business Impact Manager functions

The degradation or failure of important infrastructure elements can slow or stop vital business processes and business services, or dramatically reduce user productivity in needed business areas. VMware Smart Assurance Business Impact Manager ensures maximum availability of services.

VMware Smart Assurance Business Impact Manager (Business Impact Manager) extends the capabilities of Service Assurance to calculate the business impact of events, and to propagate the impacts to affected business entities as discrete notifications that are linked to elements in the infrastructure.

Users can create business entities, such as organizations, business units, lines of business, and departments, and relate them to corresponding infrastructure elements. Users can also create business processes.

In Business Impact Manager, users can assign different weights to any elements in the business or infrastructure topology. Business Impact Manager calculates the impact of root-cause problems by summing up the weights of the impacted elements.

The calculated impact enables operations management to prioritize notifications in accordance with business needs, and to effectively use their time and resources to resolve problems that degrade or threaten vital processes and services.

Business process tools are also provided for users to create, update, and delete events associated with their business processes. For example, a user might create an event that represents a telephone call from a supplier who is out of stock of a popular retail product, and then associate the event with the user's Order Fulfillment Business Process.

The VMware Smart Assurance Business Impact Manager User Guide includes detailed information regarding Business Impact Manager.

VMware Smart Assurance Report Manager functions

The VMware Smart Assurance Service Assurance Manager collects a wealth of notification data. To make this data available to operations personnel, Report Manager can be implemented with Service Assurance Manager.

VMware Smart Assurance Report Manager (Report Manager), which includes a Structured Query Language (SQL) Data Interface, extracts notifications by way of a Notification List from Service Assurance, passes them to an Open Database Connectivity (ODBC) driver, and stores the notification information in a relational database. The database uses a special database schema designed for VMware Smart Assurance notifications.

Notification information can then be extracted from the database, and imported into Crystal Enterprise Reports or some other user-selected report application.

The Report Manager includes predefined report files (in Crystal format) that can be used to display or print a wide variety of operational and management reports. The predefined report files include:

- Day-to-day operations reports
- Operations management reports
- Maintenance reports
- Business impact reports

Day-to-day operations reports

The notification data stored by Service Assurance can be used to generate a variety of reports that are helpful for day-to-day operations. For example:

- An open event report that lists all active events, sorted by duration
- A critical customers report that summarizes availability by customer and highlights those customers with the lowest availability
- A critical devices report that allows operations management to review operations performance and identify hot spots in the infrastructure (from a failure perspective)

Operations management reports

The notification data can be used to generate management reports that provide high-level views of service quality and staff performance. For example:

- An operator workload report that lists the workload of operators through their ownership of active notifications
- A post mortem report that lists recently cleared events, sorted by duration
- An acknowledged events report that lists active, acknowledged root-cause events
- An unassigned events report that lists events that no one owns
- All active and inactive events for a specific element, showing the overall health of the element

Maintenance reports

The reports can be used to help identify problem equipment. For example:

- An availability report that summarizes the availability of all devices or just the devices of a specified class
- A recurring problem report that lists those events with the most occurrences or greatest total impact for a period of days, and highlights the most affected elements

Business impact reports

VMware Smart Assurance Business Impact Manager users also have predefined reports that track critical business entities in the network. For example:

- A critical business users report that shows the availability of devices by customer

A critical business processes report that shows the availability of a customer's business processes
VMware Smart Assurance Business Dashboard functions

The VMware Smart Assurance Business Dashboard (Business Dashboard) displays views normally available from the Global Console as a collection of VMware Smart Assurance viewlets within your organization's web page or a third-party web portal. VMware Smart Assurance viewlets can display a variety of information including a Notification Log, Status Table, Map, Summary, Notification Properties, or Containment view. Viewlets can also be customized to suit your needs. For example, a map viewlet can be set up to show a specific topology instance as the focus of the map display.

Furthermore, the viewlets can function as sources for broadcasting context information to other, listener viewlets. For example, a Status Table viewlet and a Notification Log viewlet can be displayed such that selections in the Status Table result in the Notification Log showing notifications related to those Status Table selections.

Implementation Scenarios

4

This chapter includes the following topics:

- Challenges of network management
- VMware Smart Assurance solutions
- Enterprise provider
- Network service provider

Challenges of network management

Regardless of the business area, network management organizations everywhere are faced with the following challenges:

- Improve service
- Reduce operational costs
- Integrate new tools with existing management and support systems
- Deliver a high return on investment

VMware Smart Assurance solutions

The features and functions of the VMware Smart Assurance solutions, which include VMware Smart Assurance IP Availability Manager, VMware Smart Assurance IP Performance Manager, VMware Smart Assurance Application Services Manager, VMware Smart Assurance ATM/Frame Relay Manager, and VMware Smart Assurance Service Assurance Manager, address important challenges that network management organizations face on a day-to-day basis.

Fast and accurate fault isolation

VMware Smart Assurance uses comprehensive topology models to quickly and accurately analyze and isolate failures in networks of any size and complexity.

VMware Smart Assurance analysis improves service by greatly reducing manual problem isolation, which accounts for up to 80 percent of total downtime. The analysis also lowers operational costs by reducing the human effort involved in isolating problems, as well as the effort involved in chasing down all the symptomatic events and false alerts.

Automated corrective actions

Once a fault has been accurately isolated, Service Assurance Manager can be configured to initiate automated responses to correct soft faults or to reroute services around failures. Because VMware Smart Assurance can separate root-cause problems from symptomatic events and false alarms, actions are only invoked when or where needed. With the VMware Smart Assurance topology models, corrective actions can be invoked against both the failed component or any impacted services.

Service Assurance Manager's automated actions avoid service downtime and provide virtually immediate service restoration. They can also improve service by fixing problems before users become impacted.

Business focus

VMware Smart Assurance Business Impact Manager can import business information directly from existing data sources such as provisioning systems. During its analysis, it places infrastructure problems in their proper business context and analyzes their impact on services, business processes, and customers. This enables managers to focus their efforts on the problems with the highest business impact.

Integration

VMware Smart Assurance solutions are designed to integrate with management tools and other operational support systems. VMware Smart Assurance leverages management data from third-party sources while providing console access to third-party management applications.
VMware Smart Assurance software's ability to distill countless events into a concise set of defined problems and exceptions makes it a natural integration point for problem management (ticketing) systems.

Service Assurance's integration with other management applications lowers operational costs by providing users with a single, consistent, intuitive interface for viewing all management data. At the same time, Service Assurance improves operational control by presenting a concise display of network problems in their full topology context, complete with their impacts and histories.

Rapid deployment and low maintenance

VMware Smart Assurance solutions are designed for rapid deployment and low maintenance. Unlike other management solutions, VMware Smart Assurance software's comprehensive set of problem and impact models automatically adapt to the configuration of the network infrastructure — providing immediate results. This same adaptability enables VMware Smart Assurance solutions to automatically keep pace with future changes in the infrastructure without the need for expensive ongoing code maintenance.

VMware Smart Assurance has the ability to automatically adapt to changes due to use of ICIM models that represent the various elements of the infrastructure, how they relate to one another, and how they can affect one another. VMware Smart Assurance solutions then apply these models to the discovered elements in a given network to provide problem and impact analysis specific to that network. Furthermore, customers who need additional functionality can leverage these models to build solutions that also adapt automatically to change.

This enables VMware Smart Assurance solutions to provide better return on investment than other management solutions. Benefits include:

- Automatic adaptation reduces the head-count needed to maintain the management solution
- Analysis that automatically adapts to changes in the environment and provides more accurate results, which reduces service downtime
- More accurate analysis frees up expensive engineering resources to work on more strategic initiatives

Enterprise provider

A diversified financial services firm deployed an VMware Smart Assurance Service Assurance Manager solution to help them manage their complex infrastructure as an integrated system rather than as sets of unrelated silos.

The primary concern of the financial enterprise was that more than 100 mission-critical applications were used by their business units, such as applications to monitor their exposure to interest and currency fluctuations. Basically, the enterprise had too many mission-critical applications for the network teams to track. At the same time, their network changed and evolved so quickly that the application teams could not stay abreast of the changes.

As a result, when network failures occurred, or when network maintenance was required, they had no way of knowing which applications were affected. Attempts to do this with traditional tools—where one specified network dependencies for each application—failed because of the need to manually maintain the correlation logic every time the network topology changed. If they missed a change, the correlation would fail.

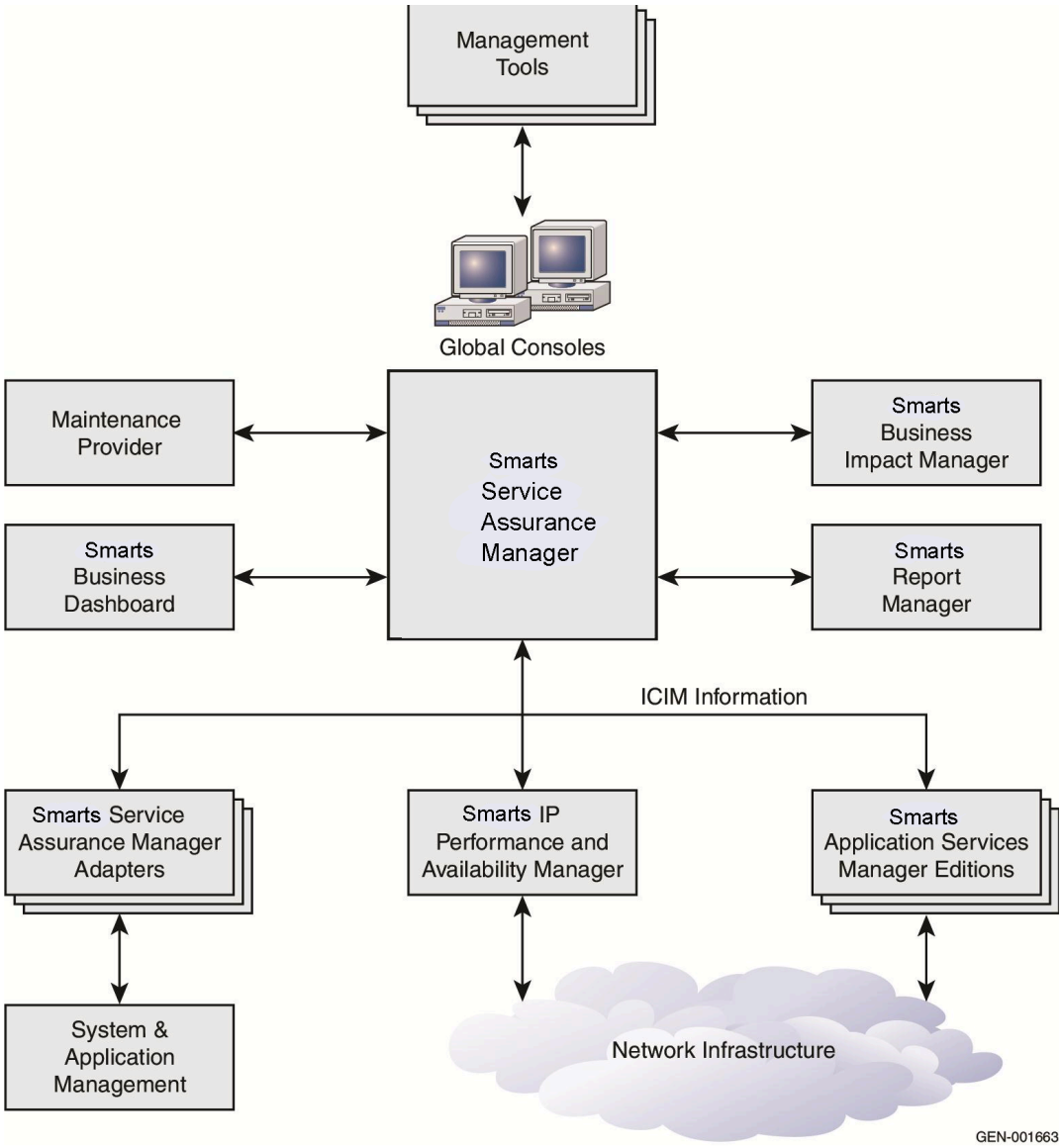
By deploying an VMware Smart Assurance solution, the enterprise was able to solve their problem by separating the network, applications, and business analysis into separate domains, thus breaking the problem into manageable pieces, as well as automating the most complicated part of their problem: defining the network dependencies of the distributed applications. Their VMware Smart Assurance solution consisted of the following:

- VMware Smart Assurance IP Availability Manager and IP Performance Manager — To monitor failures in the network infrastructure and identify the affected systems, automatically calculating the affect of any network path redundancies
- VMware Smart Assurance Application Services Manager — To perform root-cause and impact analysis of distributed applications based on events and topology information imported from the IP Availability Manager, IP Performance Manager, and the SAM adapters

- VMware Smart Assurance Business Impact Manager — To correlate failures in the technology infrastructure to the businesses they impact (for example, processing on NASDAQ trades)
- VMware Smart Assurance Service Assurance Manager — To bring it together into a single system, where users can customize views of the data they need, and use the appropriate tools to quickly restore service
- VMware Smart Assurance Business Dashboard — To provide web-based, personalized views for business unit managers (for example, in the foreign exchange unit) showing a map representation and a summary view of the status of their systems.

Enterprise solution illustrates their VMware Smart Assurance implementation.

Figure 4-1. Enterprise solution



By connecting the analysis from the network, application, and business domains, VMware Smart Assurance Service Assurance Manager provided the enterprise with an end-to-end view of causes and impacts — automatically correlating network failures with their impacts on applications and critical business processes. For example, it showed that a switch failure blocked access to a Solaris system that ran one of the two Oracle databases that supported their accounts receivable application. This resulted in degraded performance of the accounting application, and placed their ability to complete their quarterly financial reporting on time at risk.

By knowing the business impact of each problem, the operations staff effectively prioritized their support efforts on the most critical problems; that is, they aligned their efforts with the overall business objectives of the enterprise.

At the same time, because VMware Smart Assurance IP Availability Manager and VMware Smart Assurance IP Performance Manager automatically adapt to changes in the network topology, operations did not need to devote teams of people to modify the analysis every time the network topology changes. This dramatically reduced the cost to maintain their management systems. In fact, because all of the logic is based on the infrastructure topology, they only needed to manually maintain the business and application elements. VMware Smart Assurance software automatically adapted everything else: root-cause and impact analysis, personalized views, and so forth.

In addition to solving the problem of application and business impact, the VMware Smart Assurance Service Assurance Manager also streamlined operational processes.

By identifying the root causes, the support staff eliminated most of the time-consuming fault isolation process and immediately proceeded to problem resolution. By identifying which events are impacts of other problems, the support staff avoided wasting time trying to chase down and fix symptoms of other problems. Finally, by relating the root causes with the impacts, operations staff streamlined communications. For example, when estimating the time to resolve a root-cause problem, that information was automatically propagated to all affected systems, applications, and business processes.

Because they identified the actual root-cause failures (for example, a card on a switch), they were able to automate the dispatch of service technicians from their maintenance provider. More importantly, because they positively identified the failed element, they avoided the delays caused by technicians who arrived on site with the wrong parts.

By integrating the VMware Smart Assurance solution with their existing system and application management tools (by way of SAM adapters), the enterprise was able to leverage their previous investments in management tools and accelerate the deployment of the overall solution.

Network service provider

A large network service provider had been using traditional management tools to manage a broad array of services. After several years of deployment and custom work, the systems were starting to improve network operations. However, the maintenance costs were spiraling out of control and it was becoming more difficult to keep up with changes in the managed environment. Worse, the operational

improvements were not translating into higher customer satisfaction because of communications failures between operations and the call center. The provider needed to find an alternative that could deliver real improvements to customer satisfaction while reducing operational costs. The answer to this challenge was an VMware Smart Assurance solution composed of:

- VMware Smart Assurance ATM/Frame Relay Manager
- VMware Smart Assurance IP Availability Manager
- VMware Smart Assurance IP Performance Manager
- VMware Smart Assurance Application Services Manager
- VMware Smart Assurance Service Assurance Manager Adapter Platform
- VMware Smart Assurance Business Impact Manager
- VMware Smart Assurance Service Assurance Manager
- VMware Smart Assurance Business Dashboard

With the autodiscovery feature of VMware Smart Assurance autodiscovery, built-in analysis, and policy-based management, operations was able to immediately identify and isolate root-cause failures in their networks. Because VMware Smart Assurance applications automatically detect and adapt to changes in topology, the service provider no longer needed to dedicate teams of consultants to maintain them. Also, because VMware Smart Assurance intelligently manages networks with overlapping IP addresses (for example, private IPs), the provider could discontinue the expensive process of dedicating a separate management system to each customer. These features helped the provider to dramatically reduce the cost of managing their environment.

By integrating the VMware Smart Assurance solution with existing management tools (for example, system and application agents from Concord), the service provider was able to use its existing investments to cut deployment time.

The unique capability of VMware Smart Assurance to integrate not just events, but events in the context of a comprehensive topology, allowed the service provider to more effectively integrate operations with its other OSS applications. By integrating with their provisioning system, the provider was able to automatically build their business topology, and relate customers to services and services to elements in their network topology. This integration provided automated business impact analysis for prioritization, and allowed users to view technology failures in their complete technical *and* business context.

Leveraging this business topology, VMware Smart Assurance was able to automatically identify which events customers would care about so that the call center could focus on customer impacts rather than sifting through masses of arcane infrastructure events. Similarly, by using the customer data to integrate with the CRM application, VMware Smart Assurance was able to identify the account managers associated with each customer impact, and notify them of problems in real time. Furthermore, the operations staff used this information to coordinate maintenance work with the account managers of potentially affected customers.

Because problem causes and impacts were linked, the provider was also able to streamline communications between operations and the call center. For example, when operations identified a problem and dispatched an engineer to resolve it, they could estimate a repair time and the system automatically relayed that estimate for all customer impacts to the call center and customer web applications so that everyone immediately knew when the service would be restored. Finally, when customer relations faced a crisis and the customer assurance staff elevated the priorities of specific customer impacts, VMware Smart Assurance automatically applied the priority changes to the root-cause failures and notified engineering management so that operations could shift their activities accordingly.

With the Business Dashboard, the provider's customers were able to get real-time views of their data. Because these views use the same topology, the views changed automatically whenever the topology changed. This, too, reduced the cost of servicing customers.

In conclusion, by effectively integrating the VMware Smart Assurance solution with its existing applications (for example, provisioning, CRM, and call center), the service provider was able to show a more professional face to its customer. In the past, customer calls to the call center typically resulted in an operator taking messages, calling around operations to see what was happening, and then calling the customer back — a time- consuming process that often left the customer wondering what the provider was doing. Now, when the customer calls, the call center is not only aware of the problem, but is also able to give the customer up-to-the-minute information about the status of the problem and its resolution.