ServiceWatch

User Guide

Version 3.62

January 2015

Contact Information

For customer support:
http://www.servicenow.com/support/contact-support.html

For all other purposes:
http://info.servicenow.com/contact-us

Table of Contents

List of Figures and Tables

List of Figures

List of Tables

Chapter 1: Getting Started

This chapter contains the following topics:

Introduction to ServiceWatch

ServiceWatch facilitates management of business services in a dynamic, virtualized IT environment. ServiceWatch detects problematic events that impact your business services so that you can correct problems and maintain the health of the entire system.

Advantages of ServiceWatch

An essential task of IT departments is to monitor business services and intervene to ensure their availability when necessary. This requires the use of effective BSM tools.

Today, all large IT management vendors provide tools to support BSM. However, these tools all have two major drawbacks:

- The discovery process of these tools is infrastructure oriented rather than business service oriented.

  Current discovery solutions discover the infrastructure but require the user to manually define the components that belong to a business service. This manual process is time consuming and tedious. Furthermore, the manual process is not reusable and cannot be reapplied when future changes are detected.
- These tools are usually based on a static map and are not equipped to deal with the continuous changes that characterize virtualized data centers.

  While current BSM tools can be effective in a relatively static IT environment where changes are the exception, they fail to provide a robust solution in dynamic virtualized data centers where changes are common because they depend on continuous and intensive manual effort to maintain an updated service model.

ServiceWatch is the only BSM solution that overcomes these drawbacks:

- During the configuration stage, ServiceWatch performs a top-down discovery process for each business service according to business service entry points defined by the administrator. An entry point is where the end user receives the service and points to the first tier application on a host. It is the starting point from which discovery is performed in that application.
- With ServiceWatch, discovery is not a one-time affair. ServiceWatch continues to automatically perform discovery for the business service and receives events from VM managers to ensure that the topology is up-to-date, even in a virtualized environment.

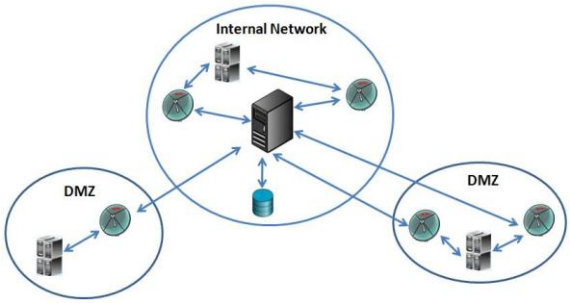
ServiceWatch does not replace the event management and monitoring tools currently installed in your IT environment. Instead, ServiceWatch integrates with them to provide a dynamic Business Service Management picture of events. In addition to providing top-down discovery and a real-time updated topology for each business service, ServiceWatch provides the following advantages:

- Agentless installation; easy to install and maintain
- Dynamic centralized deployment
- Management by exception – eliminates clutter and irrelevant data
- Minimal security requirements; passwords are user-specific, not application-specific
- Enables the IT department to evaluate the level of service provided to clients
- Enables the IT department to optimize its investment in infrastructure and resources
- System health and key performance indicators can be monitored via hand-held devices
- A 'dependency' search mechanism facilitates planning and scheduling changes
- Synthetic (user experience) monitors periodically emulate user behavior to detect usage problems
- An graphic Excel-based report generator facilitates the creation of user-defined reports

On-Premise ServiceWatch Architecture

Figure 1 illustrates the ServiceWatch on-premise architecture when the application is installed locally. The on-premise installation is described in Chapter 2.

Figure 1: ServiceWatch Architecture – On-Premise Installation



The architecture and installation of ServiceWatch as a Service in the ServiceNow cloud is described in Chapter 3.

Main Components

The main components of ServiceWatch are:

- ServiceWatch Server – A single server  manages the entire site.
- ServiceWatch database – ServiceWatch uses a PostgreSQL database  . It can reside on the same machine as the ServiceWatch server or on a different machine.

- Collector(s) – Collectors  perform the actual discovery on the appropriate machines  . ServiceWatch submits discovery information requests (collection tasks) about machines, applications, hosts, network components, etc., to collectors. The collectors collect the information for ServiceWatch to analyze and use.

A collector has two major components:

- Main collector component
- WMI collector for Windows

At least one collector is required but you can install multiple collectors. Why multiple collectors can be advantageous is explained in ADVANTAGES OF MULTIPLE COLLECTORS. No machine can have more than one collector installed on it. It is possible to install a collector on the ServiceWatch Server machine.

You identify the IP address ranges of each machine that each collector covers. ServiceWatch submits collection tasks to the appropriate collectors by IP address. If no IP address range is specified for a collector, all collection tasks can be submitted to it.

Component interaction during Discovery

The discovery process works as follows:

- Each collector periodically polls ServiceWatch for discovery collection tasks.
- ServiceWatch submits collection tasks to the appropriate collector(s) by IP address range.
- Collectors collect the information and send the results to ServiceWatch.

Note: A collector that is disconnected can neither poll nor collect information.

- ServiceWatch analyzes the collected information and stores it in its database.
- ServiceWatch uses this information to keep the topology up to date and monitor your business services.

Advantages of Multiple Collectors

There are several reasons why you may want to install multiple collectors:

- Security – Your network may have separate DMZs and you want the ServiceWatch server to communicate with them without opening a large number of network ports. You can install different collectors in each DMZ and provide different IP ranges for each one.
- Scalability – If a network segment or area has many machines, you can install several collectors in that segment and assign the same IP address ranges to all of them. Collection tasks for that segment will then be distributed among the collectors in that segment. A collector can support up to 5000 machines.
- A Windows collector can handle any OS. However, a collector on Linux cannot handle Windows.

Where to Go From Here

This guide contains information that you need to know to effectively use ServiceWatch. The chapters in this guide are in the sequence that you should read them.

These chapters provide background information, installation instructions, and instructions for starting ServiceWatch and using its GUI.

- Chapter 1: Getting Started provides an introduction to ServiceWatch and its architecture and tells you where to go for information about specific tasks.
- Chapter 2: Installing ServiceWatch describes prerequisites and provides instructions for installing the on-premise version of ServiceWatch on Windows and Linux.
- Chapter 3: ServiceWatch as a Service describes the ServiceWatch 'in the cloud' version.
- Chapter 4: Starting & Using ServiceWatch describes the ServiceWatch user interface and System Health screen and explains how to start and stop ServiceWatch services.

Chapters 5, 6 and 7 explain how to configure global parameters, Business Services and Events.

- Chapter 5: Settings provides instructions for defining and setting Knowledge Base, General, User management and System parameters.
- Chapter 6: Configuring Business Services explains how to define business services, technical (virtual) business services and business groups, and perform root cause and impact analysis.
- Chapter 7: Configuring Events explains how to map Event Management System alert data to ServiceWatch so that ServiceWatch can display that data and issue business service alerts.

After ServiceWatch is set up and configured, it monitors your business services using dynamically updated current topology and warns you of potential problems so you can intervene if necessary.

Chapters 8 - 13 explain how to use the ServiceWatch Monitor facility to monitor your business services, how to use the History facility to analyze problems that arise, how to monitor the health of communication paths, how to design and generate reports, and how to troubleshoot problems.

- Chapter 8: Monitoring Business Services provides information about monitoring and viewing key performance indicators and the health of your business services.
- Chapter 9: Viewing Business Service History and displaying topology changes.
- Chapter 10: Monitoring Networks provides information about defining, displaying, and checking the health of the communication paths between network components.
- Chapter 11: Storage Paths explains how to define and display storage paths.
- Chapter 12: Reports describes ServiceWatch built-in and user-defined reports and explains how to create reports using the Excel Reports Generator.
- Chapter 13: Troubleshooting recommends actions that can solve some typical problems.
- Appendix A: Discovery Workflows describes the ServiceWatch discovery process.

Note: If your site uses unsupported third-party or in-house applications, you may have to manually define needed entry points, configuration items, and discovery patterns. For instructions, see the *ServiceWatch Customization Guide*.

- Appendix B: Schemas for Tables & Views lists built-in table and view schemas that can be used for ServiceWatch reports
- Appendix C: Glossary defines special terms and acronyms used in this document.
- Appendix D: Adding HTTPS Support describes how to enable HTTPS support.
- Appendix E: ServiceNow CMDB Integration describes how to use ServiceWatch with an existing ServiceNow Configuration Management Database.

Chapter 2: Installing ServiceWatch

This chapter contains the following topics:

- Installation Prerequisites
- On Premise Installation Procedure

Notes:

- For a description of the components and concepts that are relevant to installation, go to ON-PREMISE SERVICEWATCH ARCHITECTURE in CHAPTER 1: GETTING STARTED.
- Before you install ServiceWatch, ensure that all prerequisites have been performed. After you have satisfied the prerequisites, you can run the installation.

Installation Prerequisites

Before beginning the installation, perform the following prerequisites:

- Ensure All Hardware & Software Requirements Are Satisfied
- Plan Your Collector Configuration
- Create Your Own ServiceWatch Database (if needed)

Ensure All Hardware & Software Requirements Are Satisfied

Minimum hardware and software requirements:

- For the Server:
  - ✓ Memory: 4 GB RAM for the server , 1 GB RAM for the collector
  - ✓ CPU: 2+ GHz processor
  - ✓ Disk space: 1000 GB HD, 20 GB for the collector
  - ✓ Reserve port 8080 for the ServiceWatch server. No other software should use it.
  - ✓ OSs for Servers and Collectors:
    - Microsoft Windows 2008 or higher
    - RedHat Enterprise Linux 5 or higher
    - Oracle Linux
    - Debian Linux
    - Ubuntu Linux
- For Windows machines that have collectors:
  - ✓ .NET Framework version 3.5 SP1

Plan Your Collector Configuration

Apply the information presented in ADVANTAGES OF MULTIPLE COLLECTORS on page 18 to your site's specific processing requirements to determine:

- how many collectors to install
- where to install them
- what IP address ranges each collector should cover

Create Your Own ServiceWatch Database (if needed)

Note: This prerequisite is relevant only if you supply your own PostgreSQL database for ServiceWatch. If you will be using the ServiceNow-supplied PostgreSQL database, skip this prerequisite.

If you are *not* using the ServiceNow-supplied PostgreSQL database, ensure that the database administrator has prepared a PostgreSQL database for ServiceWatch and has given you the appropriate credentials. Otherwise, ensure that you have the following information for the PostgreSQL database: host address, port, database name, username and password.

On Premise Installation Procedure

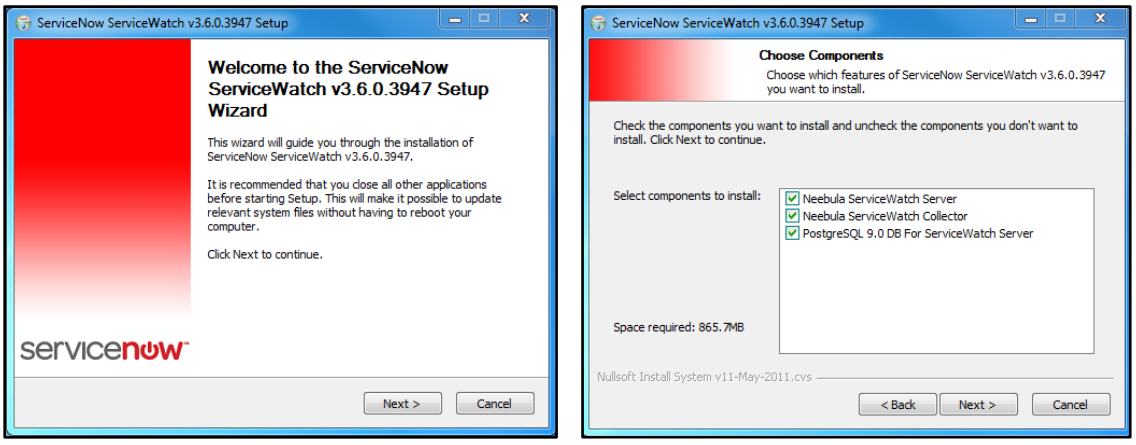
This installation procedure is required only for on-premise users of ServiceWatch. ServiceNow cloud SWaaS users should see CHAPTER 3: SERVICEWATCH-AS-A-SERVICE.

This section contains the following procedures:

Installing ServiceWatch on Windows

1. After downloading the appropriate installation files, run the **ServiceNow-ServiceWatch-<version>-setup.exe** file on the Server machine. This file runs the Install wizard.
2. Page through the wizard.

Figure 2: Installation Wizard: Welcome & Choose Commands



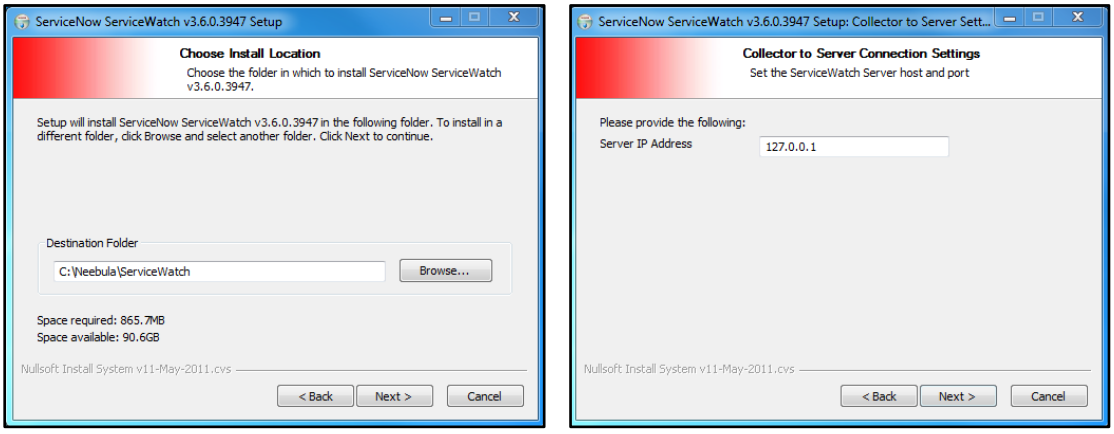
3. The **Choose Components** screen of the wizard is displayed for a new installation but not displayed for an upgrade.

- The ServiceWatch Collector checkbox is checked. If your configuration does not include a collector on this Server machine, uncheck this box.
  - ✓ For every other Windows machine where you want a collector installed, run the installation setup but be sure to choose only the Collector component in the Choose Component page.

✓ You can limit the IP ranges of collectors when you specify settings (see CHAPTER 5: SETTINGS). For instructions on defining collector IP ranges, see COLLECTORS on page 114.

The PostgreSQL database checkbox is checked. If you are using your own PostgreSQL database, uncheck this checkbox but ensure your own database is ready (as mentioned in the prerequisites).If you are using the supplied PostgreSQL and this is the first time it is being installed on this machine (not an upgrade), verify that no other PostgreSQL was installed on this machine to avoid failure of the PostgreSQL installation.

Figure 3: Installation Wizard: Choose Install Location & Collector to Server Connection Settings

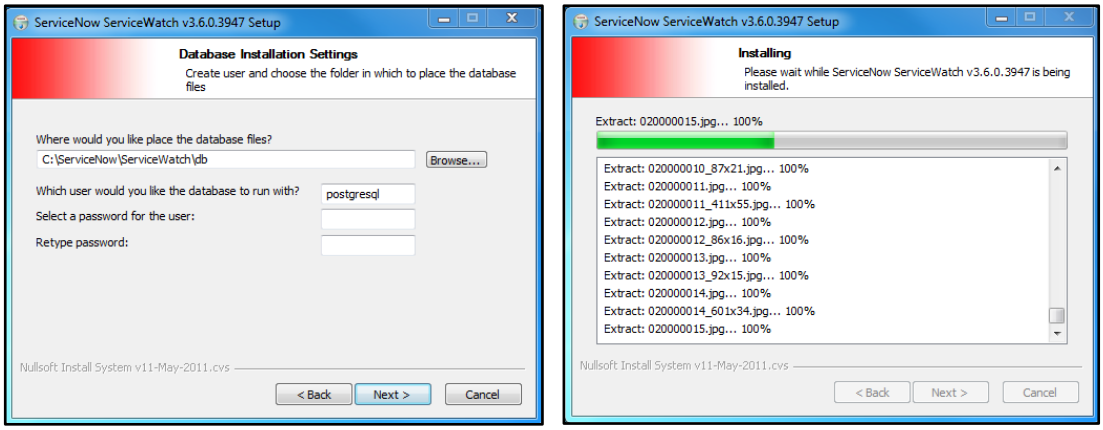


4. The **Choose Install Location** screen is displayed for a new installation but not displayed for an upgrade. If displayed, browse for the desired **Destination Folder** location and click **Next**.
5. The **Collector to Server Connection Settings** screen is displayed for a new installation but not for an upgrade. If displayed, type in the local **Server IP Address** for the server on which ServiceWatch is installed. This is the address that the collector should transmit to. If the collector is installed on the same machine as the server, specify **127.0.0.1** and click **Next**.
6. The **Database Installation Settings** screen is displayed for a new installation but not for an upgrade. If displayed, verify the database files location. The default database user is **postgresql**. Files belonging to this database are owned by this user. ***This user must also own the database server process.*** Enter and retype the password for this user.

Note: This password must comply with the organization's password policy or the installation of PostgreSQL will fail. In general, a password with 6 or more characters including at least one uppercase letter, one lowercase letter, one number and one special character would satisfy most organization's password policy.

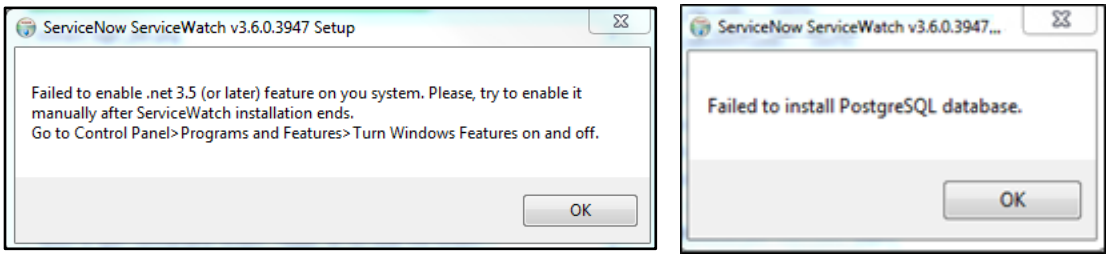
When you click **Next**, the **Installing** screen is displayed.

Figure 4: Installation Wizard: Database Installation Settings & Installing



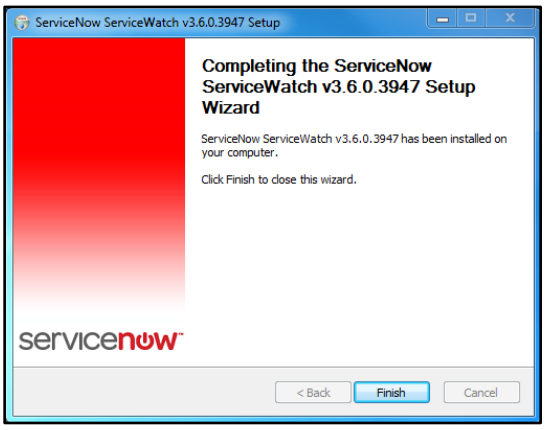
7. If the **Failed to enable .net 3.5.1 feature** message is displayed, in most cases you can ignore it. On some Windows versions, this message is displayed because the .net 3.5.1 feature is already enabled and a wrong end condition is returned from the Microsoft silent installation. You can view the Windows control panel to verify that this is indeed the case.

Figure 5: Installation Wizard: Failed to enable .net 3.5.1 & Failed to install PostgreSQL database



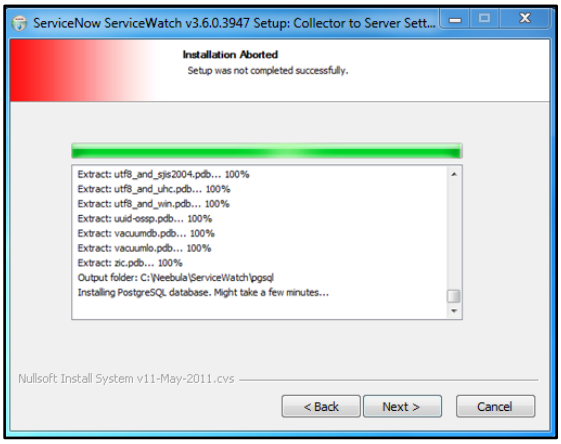
8. If a **Failed to install PostgreSQL database** message is displayed, you may have specified a database user who is not the owner of the database server process. This can happen if PostgreSQL was previously installed without using the ServiceWatch installation wizard or the password did not comply with the organization's policy. Ensure the database user is the owner of the database server process and rerun the installation with a stronger password. If you still receive this message, contact customer support.
9. You should receive a setup **Finish** screen similar to this one:

Figure 6: Installation Wizard: Finish screen

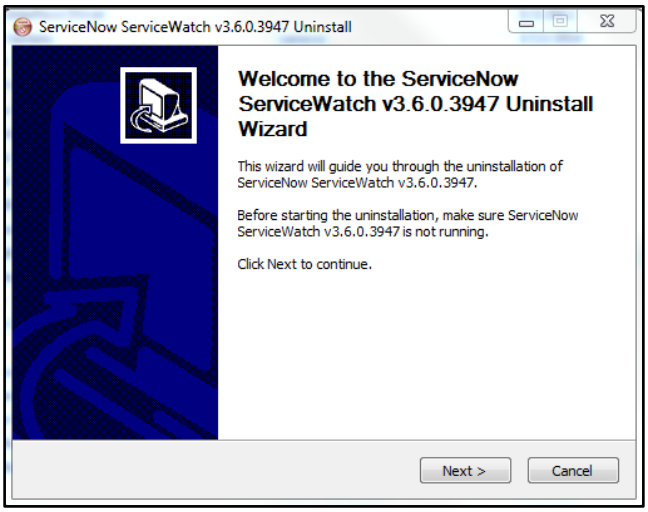


10. If you receive an **Installation Aborted** screen and cannot resolve the problem, contact ServiceWatch customer support.

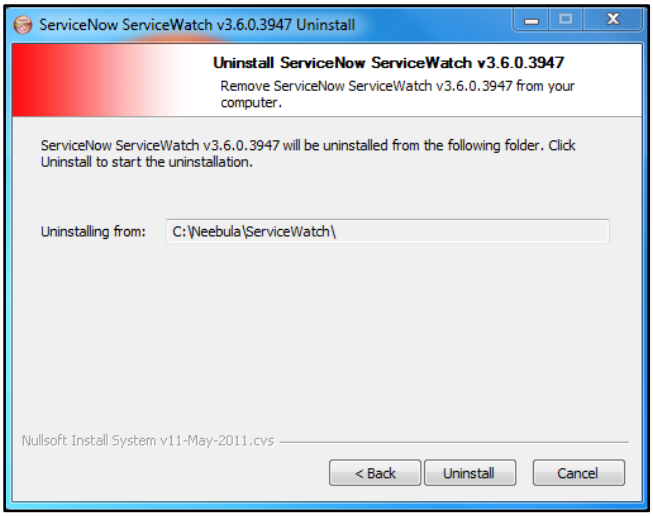
Figure 7: Installation Wizard: Installation Aborted screen



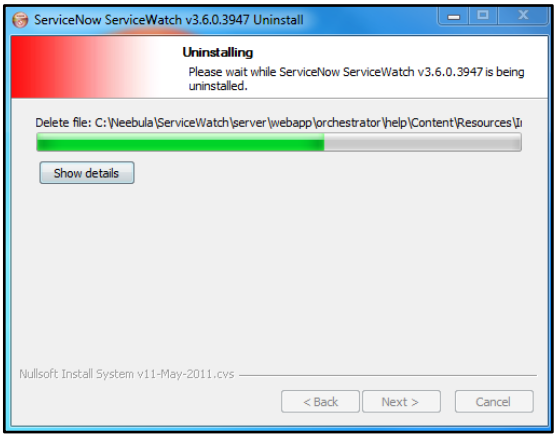
11. To uninstall ServiceWatch, use the Uninstall or change a program utility in the Windows Control Panel. When you click the Uninstall/Change button, the Welcome screen of the ServiceNow ServiceWatch Uninstall Wizard is displayed.

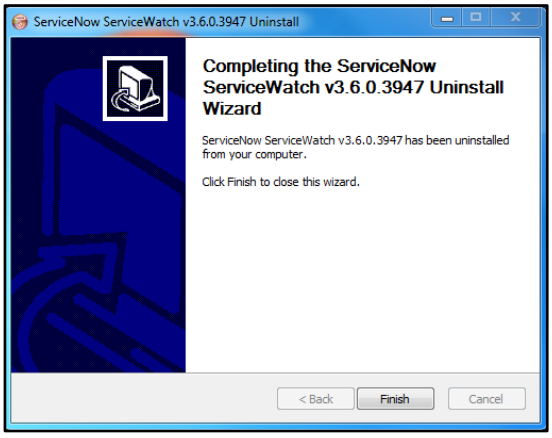


12. Click **Next**. The folder location screen is displayed.



13. Click the **Uninstall** button. The **Uninstalling** screen is displayed.





14. When the process has finished, the **Completing** screen is displayed. Click the **Finish** button.

Installing ServiceWatch on Linux

To install ServiceWatch on Linux, perform the steps described after this list of steps:

1. Unzip the Linux version of ServiceWatch zip file
2. START THE INSTALLATION BY RUNNING THE INSTALL.SH SCRIPT
3. Adding HTTPS Support

Notes:

- If you are upgrading from an earlier release, the upgrade does not require flags/arguments to be passed. If the installation script finds a previous ServiceWatch installation, it prompts the user to confirm an upgrade.
- For examples, see EXAMPLES on page 28.

Unzip the Linux version of ServiceWatch zip file

Unzip the installation file to a folder of your choice.
Lines that begin with **$** are prompts. The lines after the prompt lines are responses.

```
$  /  mkdir -p /tmp/serviceWatch
$  /  cd /tmp/serviceWatch
   ...
$  serviceWatch  unzip Neebula-ServiceWatch-v1.5.0.948-linux_i386.zip
   ...
   inflating: server/lib/thirdparty/jetty-continuation-7.1.3.v20100526.jar
   inflating: server/lib/thirdparty/axiom-impl-1.2.5.jar
   inflating: server/lib/thirdparty/com.springsource.org.aopalliance-
1.0.0.jar
   inflating: server/lib/apidata-1.0.0.jar
$  serviceWatch
```

Start the installation by running the install.sh script

You can run this file either as root or as a regular user.

Note: If running as a regular user, add **sudo** to run **install.sh**, for example
$ serviceWatch sudo ./install.sh

If running as root, login as root to run the installation.

```
root@ubuntu-virtual-machine:/tmp/serviceWatch#
```

Add execution permission to the file and execute the **install.sh** script, for example:

```
$  serviceWatch
Chmod +x install.sh
root@ubuntu-virtual-machine:/tmp/serviceWatch# ./install.sh

Neebula ServiceWatch 3.1.3.100 installation tool
```

Usage

```
install.sh [options: -C, -S, -CS, -SP or -CSP]
  --install-dir    - Installation Directory
  --user          - Username under which ServiceNow ServiceWatch will run

[Collector only options]
  --server-host       - ServiceNow ServiceWatch Server host address

[Server only options]
  --db-dir            - Directory for database files
  --database-type     - Database Type [Postgresql]
  --database-host     - Database host address
  --database-port     - Database port number
  --database-name     - Database schema name
  --database-user     - Database user name
  --database-password - Database user password
```

Examples

Example 1

Install the Collector, Server & PostgreSQL on the same machine in **/opt/neebula** with user **neebula**:

```
./install.sh -SCP --install-dir  /opt/ServiceNow
                  --user nebula
                  --database-dir /opt/neebula/db
```

Example 2

Install only a Collector with the Server on 192.168.1.13:

```
./install.sh -C   --install-dir  /opt/neebula
                  --user neebula
                  --server-host 192.168.1.13
```

Example 3

Install the Server and a PostgreSQL database

```
./install.sh -SP  --install-dir  /opt/neebula
                  --user nebula
                  --database-dir /opt/neebula/db
```

Example 4

Install the Server only with remote database connection to a PostgreSQL database host on 192.168.3.3, port 1234, named **neebula_db**, user: **neeb_db_user**, password: **pass**

```
[sudo] ./install.sh -S  --install-dir /opt/neebula
                        --user neebula
                        --database-type postgresql
                        --database-host 192.168.3.3
                        --database-port 1234
                        --database-name neebula_db
                        --database-user neeb_db_user
                        --database-password pass
```

Adding HTTPS Support

For general information about configuring SSL in a Jetty web server, see **http://wiki.eclipse.org/Jetty/Howto/Configure_SSL**

To enable ServiceWatch to provide HTTPS support and to view instructions for adding a certificate, see APPENDIX D: ADDING HTTPS SUPPORT.

Chapter 3: ServiceWatch as a Service

This chapter contains the following topics:

Note: Before using the ServiceWatch-as-a-Service wizard to create collectors and configure ServiceWatch, ensure the Installation Prerequisites on page 21 have been satisfied.

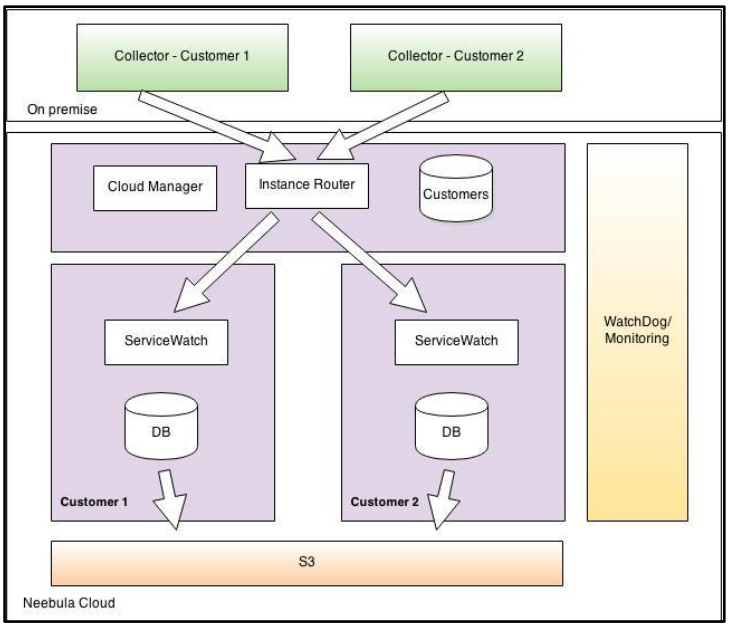
Main Components

The main components of ServiceWatch are described at Main Components on page 17. The advantages multiple collectors are listed at Advantages of Multiple Collectors on page 18.

Architecture of ServiceWatch as a Service

Figure 8 illustrates ServiceWatch as a Service architecture when the application is accessed remotely. Installing ServiceWatch as a Service in the ServiceNow cloud is described below.

Figure 8: ServiceWatch as a Service Architecture – Server & Database in the Cloud



Collector Requirements

When using ServiceWatch as a Service in the ServiceNow cloud, one or more Servers and the ServiceWatch application are accessed via the Internet using secure communication protocols. One or more collectors are installed at customer sites.

Ensure All Hardware & Software Requirements Are Satisfied

Minimum hardware and software requirements:

- For each Collector:
  - ✓ Memory: 2 GB RAM
  - ✓ CPU: 2+ GHz processor
  - ✓ Disk space: 20 GB
  - ✓ Reserve port 8080 for the ServiceWatch server. No other software should use it.
  - ✓ OS for Collectors: Microsoft Windows 2008 or higher
  - ✓ .NET Framework version 3.5 SP1

Plan Your Collector Configuration

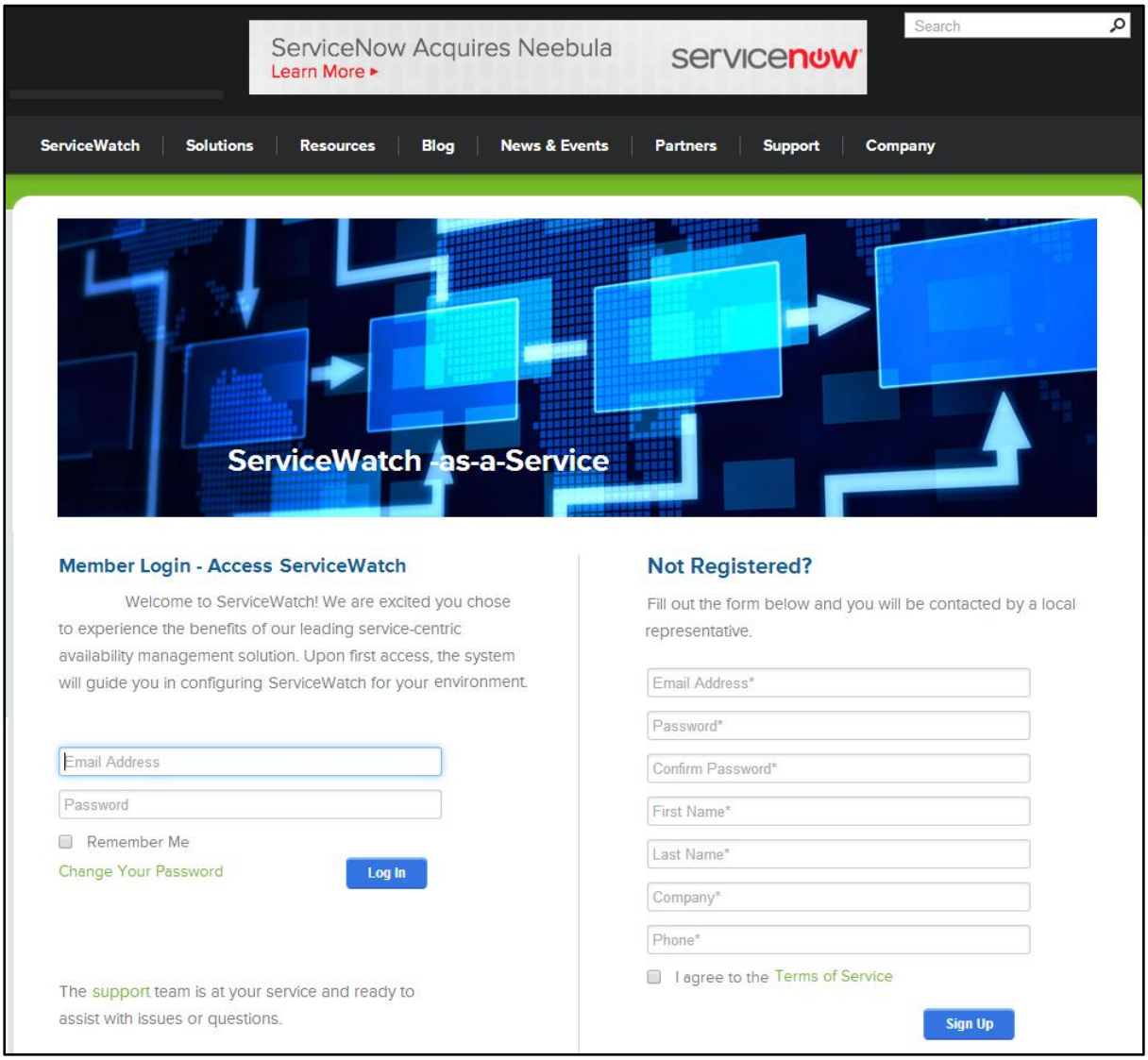
Apply the information presented in Advantages of Multiple Collectors on page 18 to determine:

- how many collectors to install
- where to install them
- what IP address ranges each collector should cover

Registration

Enter servicewatch.servicenow.com in your browser to access the ServiceWatch-as-a-Service webpage.

Figure 9: ServiceWatch-as-a-Service Registration & Login webpage



Fill in the data fields on the right side of this webpage, select the **Terms of Service** checkbox, and click the **Sign Up** button.

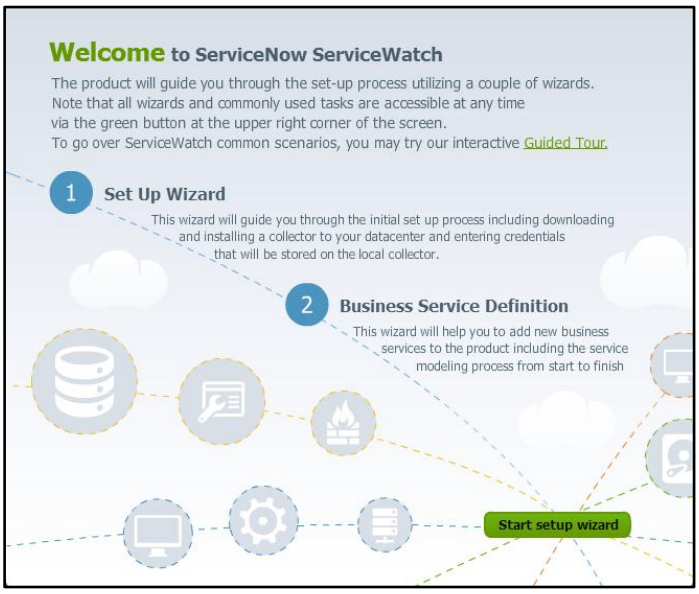
You should receive the following reply on that web page:

Thank you for registering for ServiceWatch in the Cloud

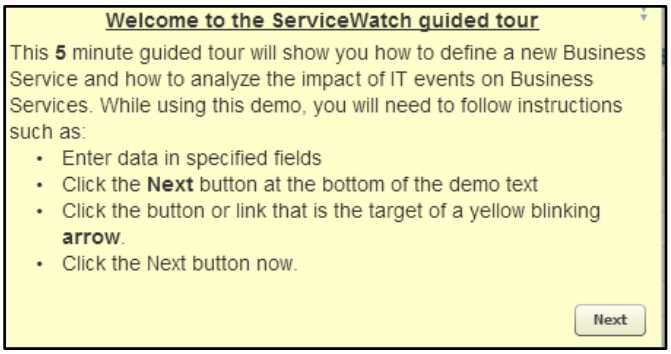
Your 30 day trial is about to begin.
We are now preparing your personalized ServiceWatch environment and you will soon receive an email with instructions on how to access it.

You should receive an email confirmation of your Registration after a few minutes. When you receive the confirmation, fill in your email address and password on the left side of the servicewatch.servicenow.com webpage and click the **Log In** button.
The following window will be displayed:

Figure 10: ServiceWatch-as-a-Service Registration & Login webpage

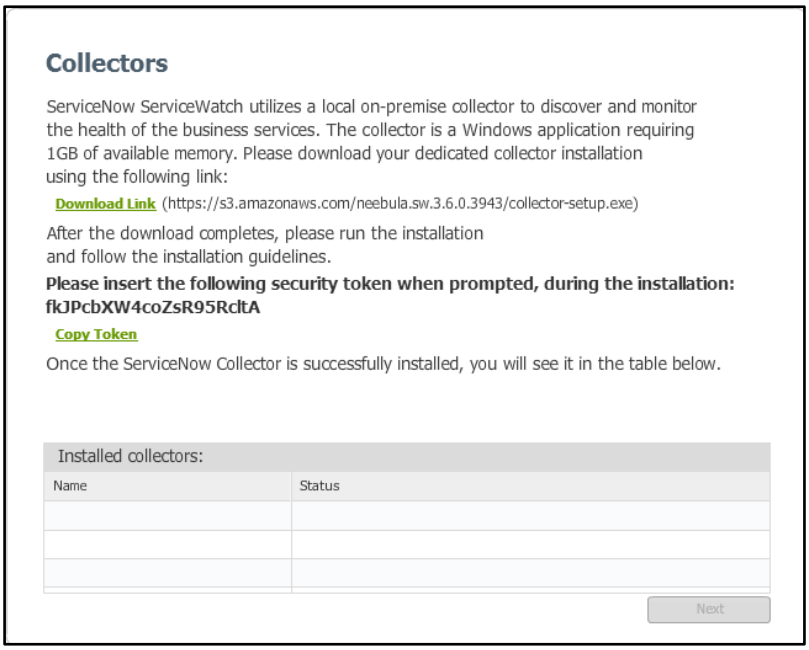


Enjoy the Guided Tour



and then click the 

button. The wizard will guide you through the following steps:

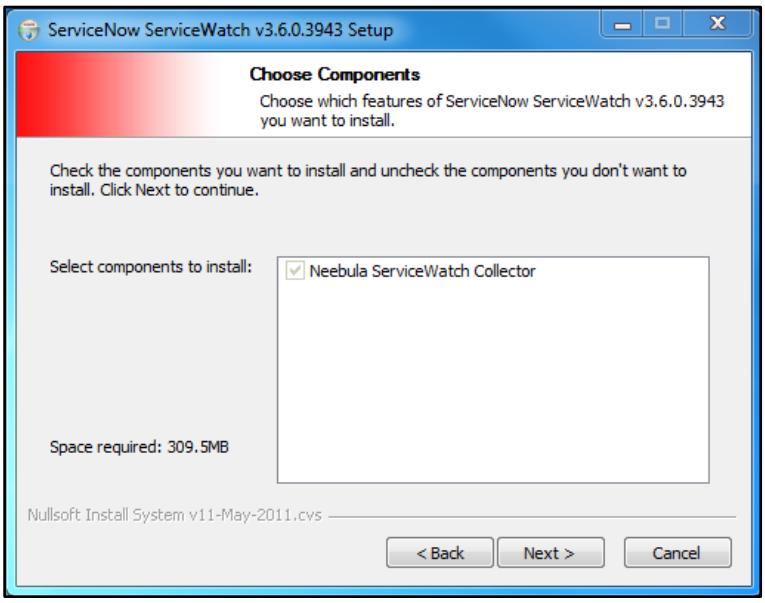


Download the Collector installation by clicking **Download link**. The **collector-setup.exe** file will download into the folder you specify. When you run **collector-setup.exe**, the Collector Installation wizard Welcome screen is displayed.

Figure 11: ServiceWatch Collector Wizard welcome screen

Click **Next** to display the **Choose Components** screen.

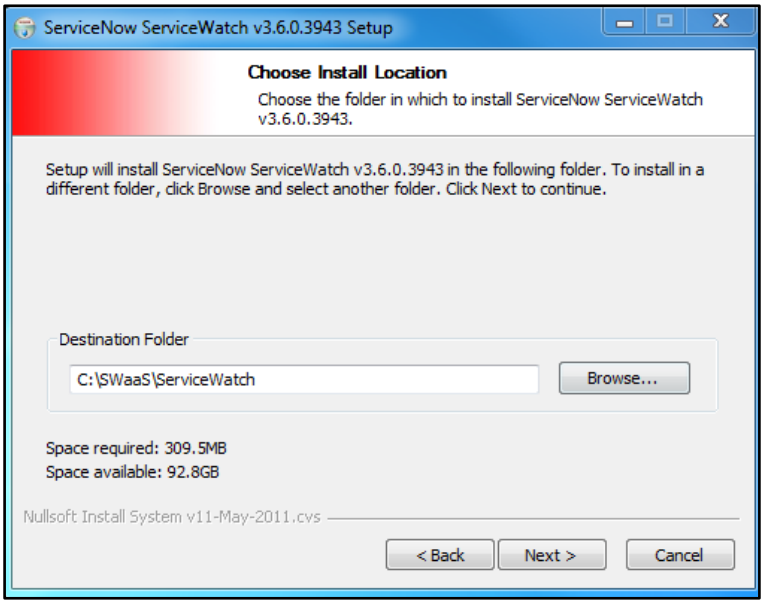
Figure 12: ServiceWatch Collector Wizard Choose Components screen



The **ServiceWatch Collector** checkbox is already selected and grayed-out. Click **Next**.

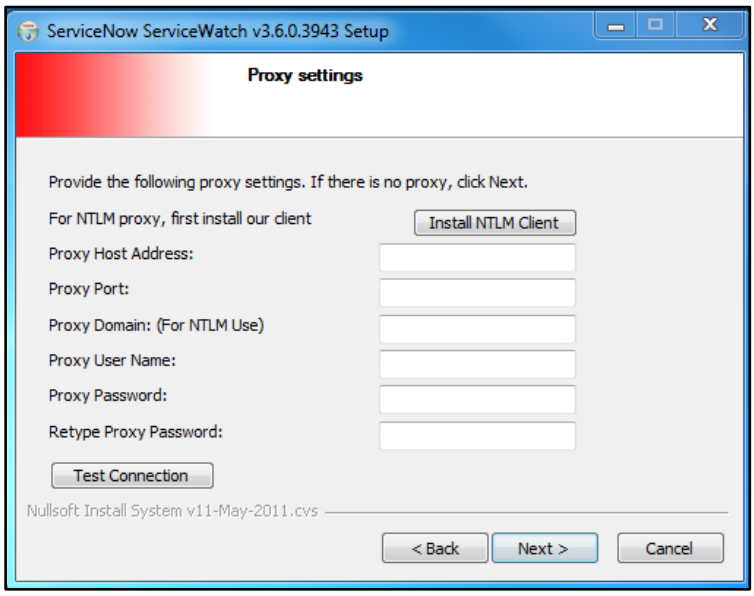
The **Choose Install Location** screen is displayed.

Figure 13: ServiceWatch Collector Wizard Choose Install Location screen



The default location is **C:\Neebula\ServiceWatch** You can optionally **Browse** for another location. Click **Next**. The **Proxy settings** screen is displayed.

Figure 14: ServiceWatch Collector Wizard Proxy settings screen



If you are *not* using a proxy, skip this screen by clicking **Next**.

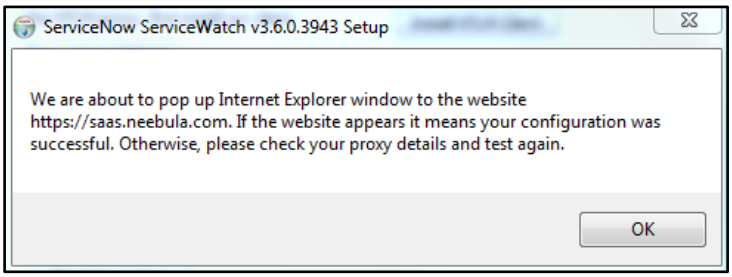
If you are using a regular proxy (not NTLM), do *not* click the **Install NTLM client** button. Skip the **Proxy Domain: (For NTLM Use)** field and fill in the other 5 fields.

If you *are* using NTLM (NT LAN Manager) authentication, click the **Install NTLM client** button to display an NTLM client installation wizard in a separate window. Follow that wizard's instructions.

After installing the NTLM client, you will automatically return to this **Proxy settings** screen. Fill in all 6 text fields. The **Proxy User Name** is the name that is used to authenticate the proxy. When using NTLM, the **Proxy User Name** does *not* include the domain name.

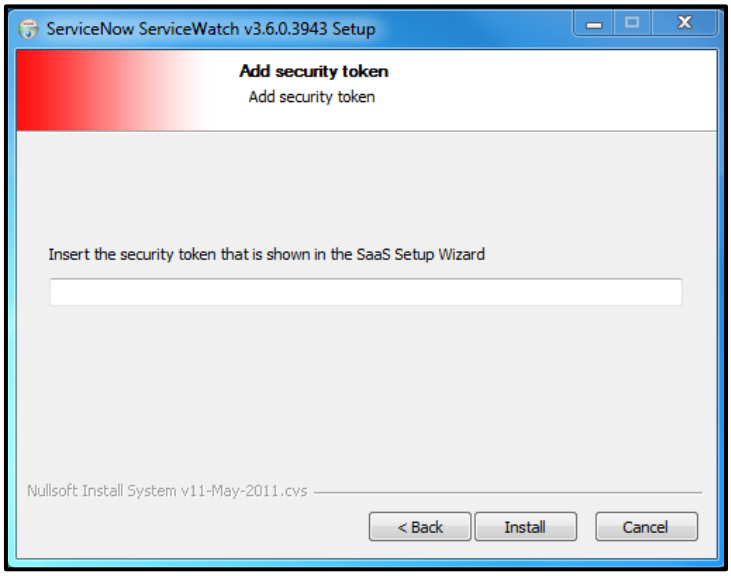
In all 3 cases (no proxy, NTLM proxy, regular proxy) you should click 

. An Internet Explorer window pop-up warning is displayed.

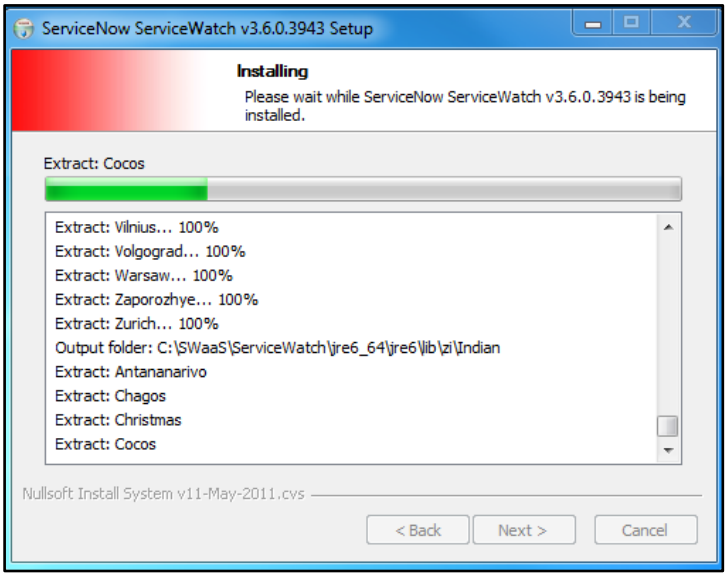


Click **OK**. If the test is successful, the https://saas.neebula.com website is displayed in an Internet Explorer window. Reduce or close the displayed website and click **Next** to display the **Add security token** screen.

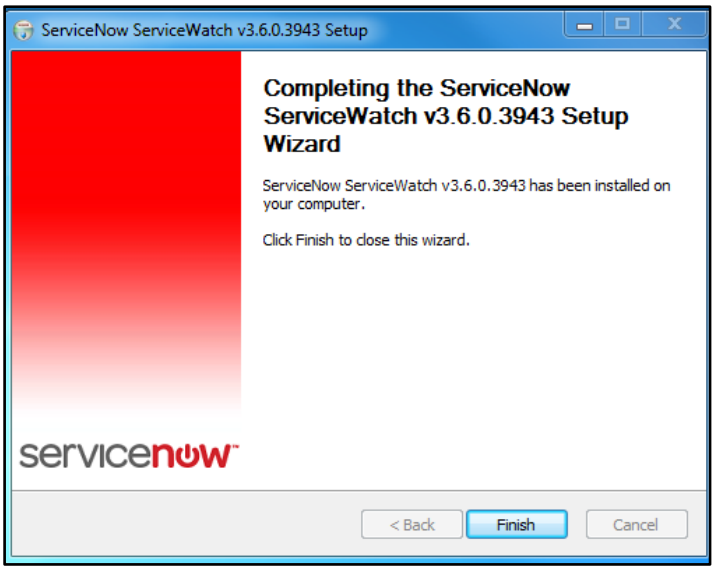
Figure 15: Add Security token screen



Insert the Security Token that was displayed in the SWaaS Setup Wizard, for example, **fkJPcbXW4coZsR95RcltA** and click the **Install** button. The **Installing** screen is displayed.

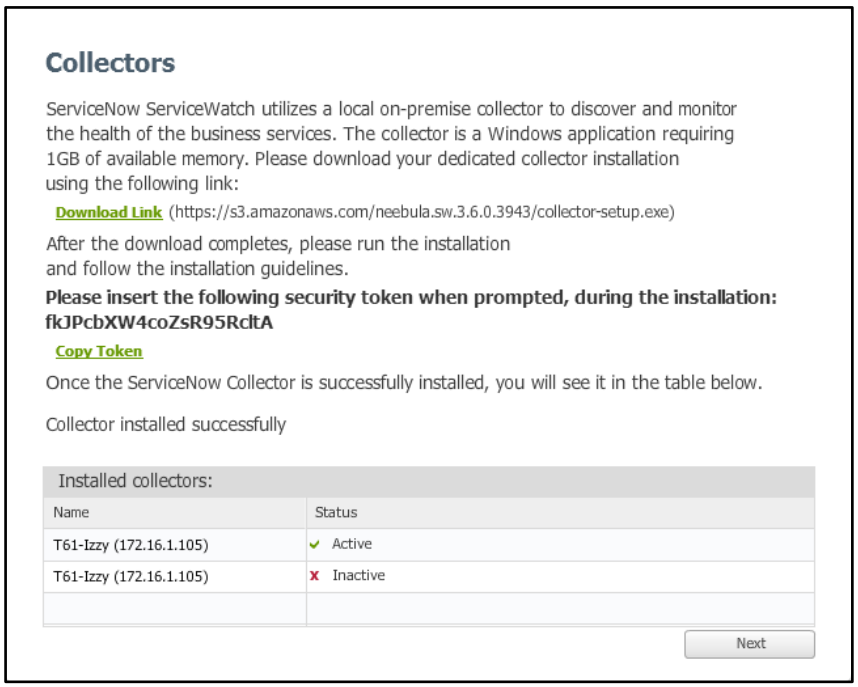


When the Collector installation finishes, the **Completing** screen is displayed.



Click the **Finish** button and examine the **Installed collectors** table to verify that the desired collectors have been installed.

Figure 16: Installed Collectors Table



Collector Configuration

Collector configuration is described under the topic Collectors on page 114.
The current health status of Collectors is illustrated in Figure 48 on page 64.

Security Assertion Markup Language

SAML support is available when using ServiceWatch as a Service. Contact Technical Support if you need this feature.

Chapter 4: Starting & Using ServiceWatch

This chapter contains the following topics:

Starting ServiceWatch

1. In your browser, enter `http://<ServiceWatchServerHostname>:8080/`
2. Enter your user name and password. Default user name: **admin**. Default password: **admin**.
   The ServiceWatch application opens and displays the current default Dashboard.

Note: Change the default user name and password and keep them in a safe place. The on-premise version of ServiceWatch has no password recovery process.

Starting and Stopping ServiceWatch Services

ServiceWatch has the following services. These services should start automatically.

- PostgreSQL database
- ServiceWatch Server
- ServiceWatch Collector
- WMI Collector

To stop or restart a ServiceWatch service, perform these steps on the machine where the service is installed:

1. From the Windows Start menu,
   (a) select the Administrative Tools utility in the Control Panel and select System and Security Services, *or*
   (b) enter **services.msc** in the **Search programs and files** text box and click **Services(Local)**.
2. In the displayed list of services, click the service(s) to be started.
   The **PostgreSQL** database service *must* be started before the Server or Collectors.
3. In the displayed operation options on the left, click the desired operation (Stop, Restart).

Integration with 3rd party tools

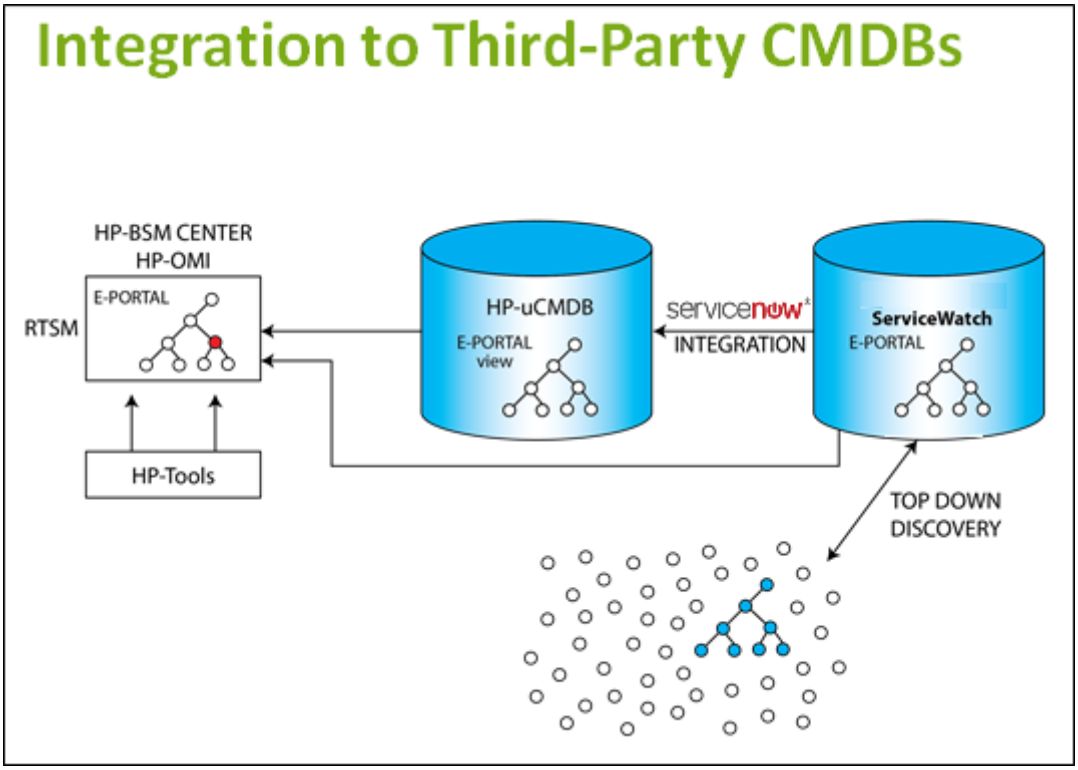
ServiceWatch integrates with other event management and monitoring tools to indicate how events impact business services. **Critical**, **Major**, **Minor**, **Warning** or **Information** severity is assigned to each event. The list of integrated products includes: GroundWork, HP Operations Manager, Netcool, SCOM, SolarWinds, Vcenter and others. Generic integration uses SNMP traps and NBLEVENT commands.

ServiceWatch has an Event binding feature that facilitates automatic binding of events as they occur. For information about this feature, see Extracting and Binding Event Information on page 173.

Service Watch integrates with Application Program Interfaces (APIs). RESTful APIs can import / export management data (users, roles, credentials, history and changes) and business service topology.

ServiceWatch also integrates with Virtualization tools and Configuration Management Databases (CMDBs) including HP uCMDB, ServiceNow, CA and BMC.

Figure 17: Integration with 3rd party HP uCMDB



Screens

Menu Bar

The **Menu** bar has 6 buttons, including a Collectors icon plus a green area in the top right corner that enables you to define a Business Service or Technical Business Service.

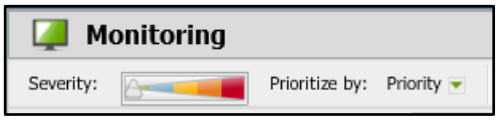
The currently active button name or Settings tool is **green**. The color of the button indicates the status of the collectors. Clicking this button displays the System Health screen.

Figure 18: ServiceWatch Menu Bar

Severity Color Coding

The color coding identifies the severity of the problem:

- CRITICAL
- MAJOR
- MINOR
- WARNING
- INFORMATION



The business service is color coded according its most severe event. For example, if a business service has a Critical event and Minor event, it is color coded as Critical. To filter the business services that are displayed in the Dashboard by severity, use the **Severity** slide near the top left corner of the Dashboard. Business services whose severity code color is located to the right of the slide will be displayed.

Screen Panels & Panes

Screen content depends on menu, tree, list and tab selections. Screens can contain:

- Active tree of active business services (in the left pane, above the Pending list)
- Pending list of inactive business services (in the left pane, under the Active tree)
- Map panel – Displays the topology of the business service selected in the Active tree (in any mode) or in the Pending list.
- Definition panel –Displays the name, group, priority, and entry points of the business service selected in the Active tree (in Edit mode) or in the Pending list.
- Properties panel – Displays properties of an object selected in a Topology Map.
- Impact Tree – Shows how a business service is affected by the status of its elements.
- Events panel – Displays events related to a selected CI or business service.
- KPI panel – Displays Key Performance Indicators of selected business services or CIs in tabular or chart mode for the previous hour, day, week or month.
- Messages panel – Displays messages of a Pending business service or an Active business service when its Map is displayed in Edit mode.
- SLA panel – Displays SLA rules for a Pending business service or an Active business service when its Map is displayed in Edit mode.
- Impact panel – Indicates effect of source severity on targets and redundancy targets.

Dashboards

Dashboard View Toggle Buttons

There are 3 view modes 

. Click  to display the **Bubble** format,  to display the **Tile** format, or  .to display the **List** format.

Group vs. Business Service Toggle Buttons

The 

buttons toggle between displaying business services or groups of business services in the **Tile** and **Bubble** formats.

Figure 19: Factory Default Dashboard

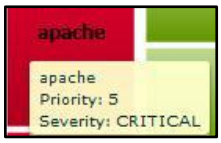
Severity Slide

In all Dashboard formats, the 

slide enables you to display only business services whose severity is higher than the slider position.

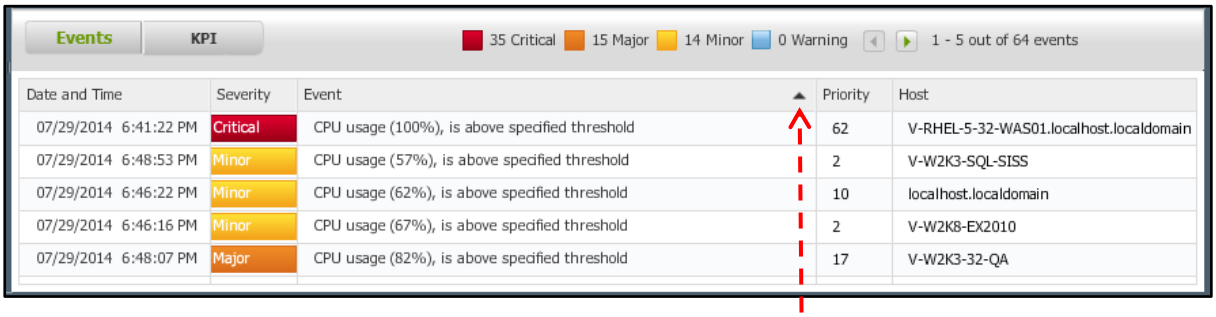
Business Services

When the cursor hovers over a business service, a tool tip indicates its <name>, Priority and Severity.



Dashboard Events

Figure 20: Events panel of the Dashboard



Events in the bottom pane can be sorted by **Date and Time**, **Severity**, **Priority** and **Host**. Clicking one of these column headers sorts the rows by that column. Clicking the same header again reverses the sort order. The current sort mode is indicated by an up or down-arrow in the column heading.

To filter events by date/time range, event state, CI name or type, or text strings and to examine event details, follow the instructions at Events window on page 50.

For events that occur during a scheduled change interval, the **Severity** level is downgraded to **Warning** and the background color of that event's row in the **Severity** column is **grey**. Events that occur before and after the change interval are displayed in the usual manner.

Event Priority

The priority of an event is displayed as a number from 0 - 100. Higher numbers indicate higher priority. Event priority is automatically calculated by a proprietary algorithm that evaluates

- the extent to which an event affects a business service
- the severity level of that business service caused by the event
- the number of business services affected by the event

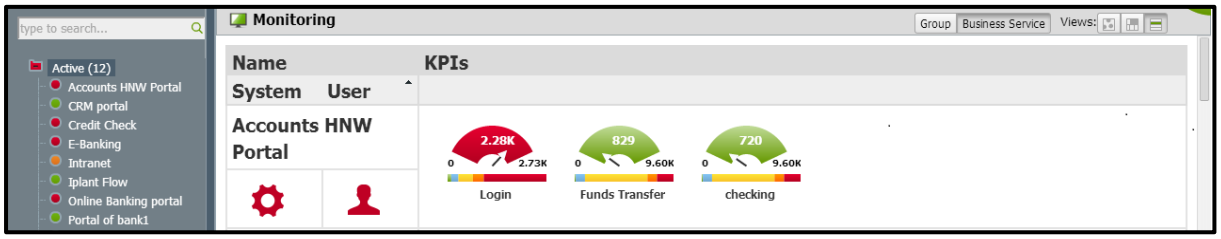
Dashboard KPIs

Click KPI to display Key Performance Indicators in the bottom pane of the Tile and Bubble Dashboards. Click any column header to sort the rows by that column. Click the same header again to reverse the sort order. The current sort mode is indicated by an up or down-arrow in the column heading.

Figure 21: KPI panel of the Dashboard

KPIs are automatically displayed in the List Format Dashboard.

Figure 22: KPIs in the List Format Dashboard



For detailed information about KPIs, see KPIs (Key Performance Indicators) on page 194.

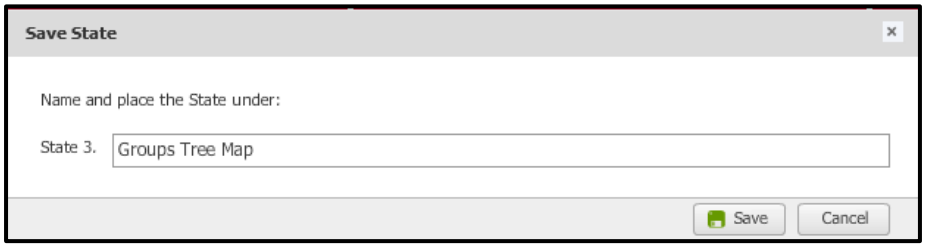
Infrastructure / User Perspective toggle button

By default, the **Monitoring** screen displays Severity levels from an Infrastructure perspective. Click to display Severity levels from a User perspective based on Synthetic (user experience) monitors and Events & KPIs that impact a business service. Click again to change the display back to the Infrastructure perspective.

Save and Load Dashboard buttons

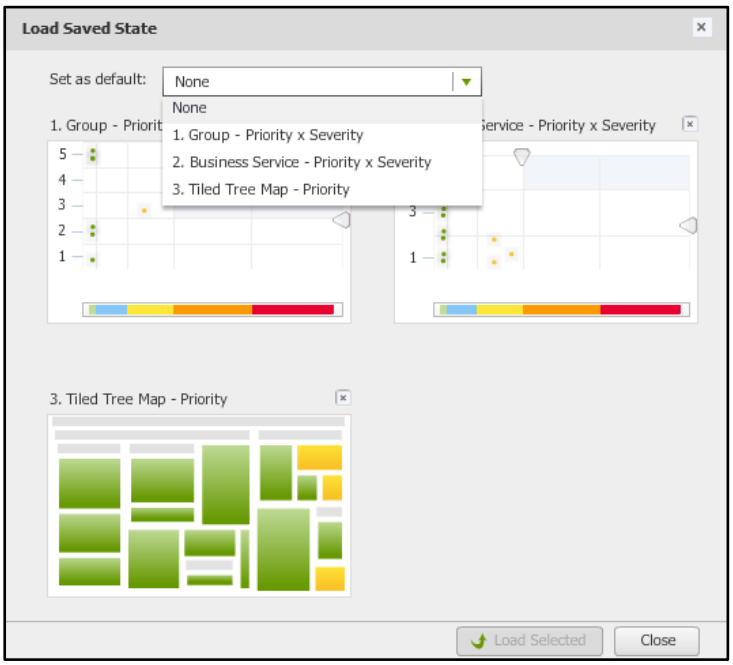
Up to 4 Dashboard formats can be saved. Clicking the Save button displays the **Save State** dialog box. You can modify the automatically displayed name in the text box. Clicking the Save button in the dialog box will save the format as State 1, 2, 3 or 4 with the specified name.

Figure 23: Saving a Dashboard format



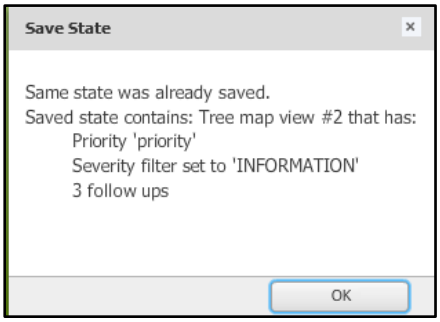
Clicking the Load button displays the **Load Saved State** dialog box.

Figure 24: Load Saved State dialog box



In this dialog box, you can select the start-up default Dashboard format from the **Set as default** drop-down list. To immediately load any pre-specified format, click that format's thumbnail image and then click Load Selected. Click Close to exit the dialog box without loading a format. If you try to save a Dashboard format that has already been saved, you will get the message:

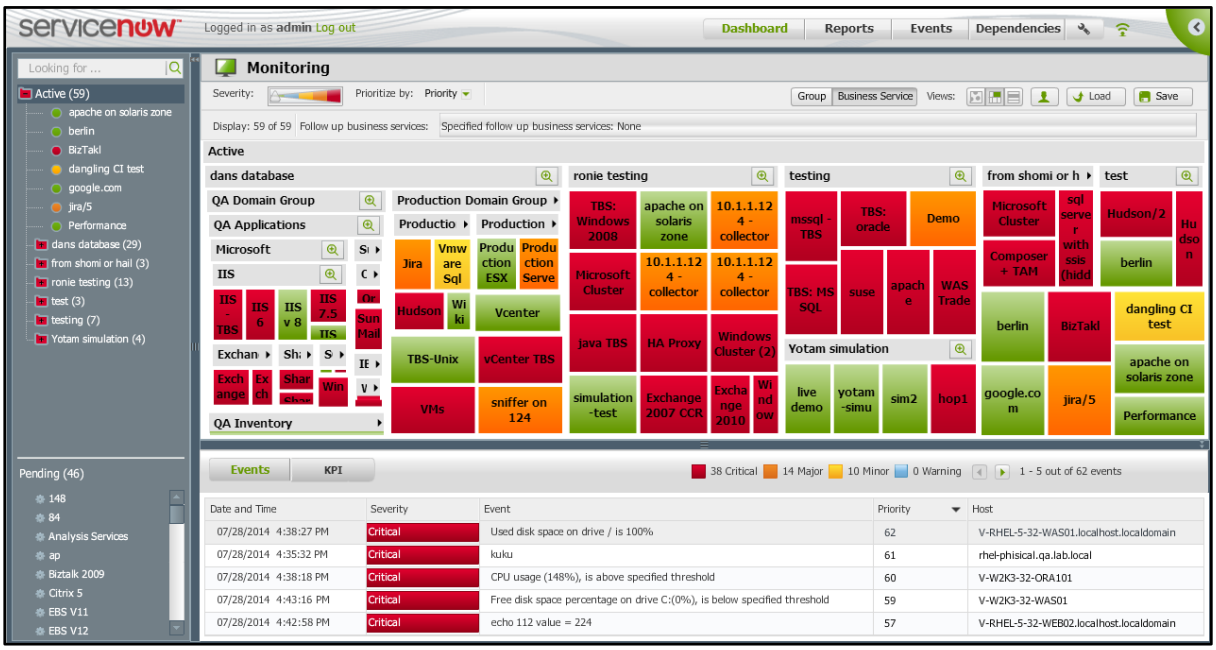
Figure 25: Save State error message



Tile Format Dashboard

Figure 26 shows a dashboard whose **Monitoring** panel for **Active** business services displays each business service or group as a tile whose size indicates its relative priority and whose color indicates its highest severity.

Figure 26: ServiceWatch Tile format Dashboard



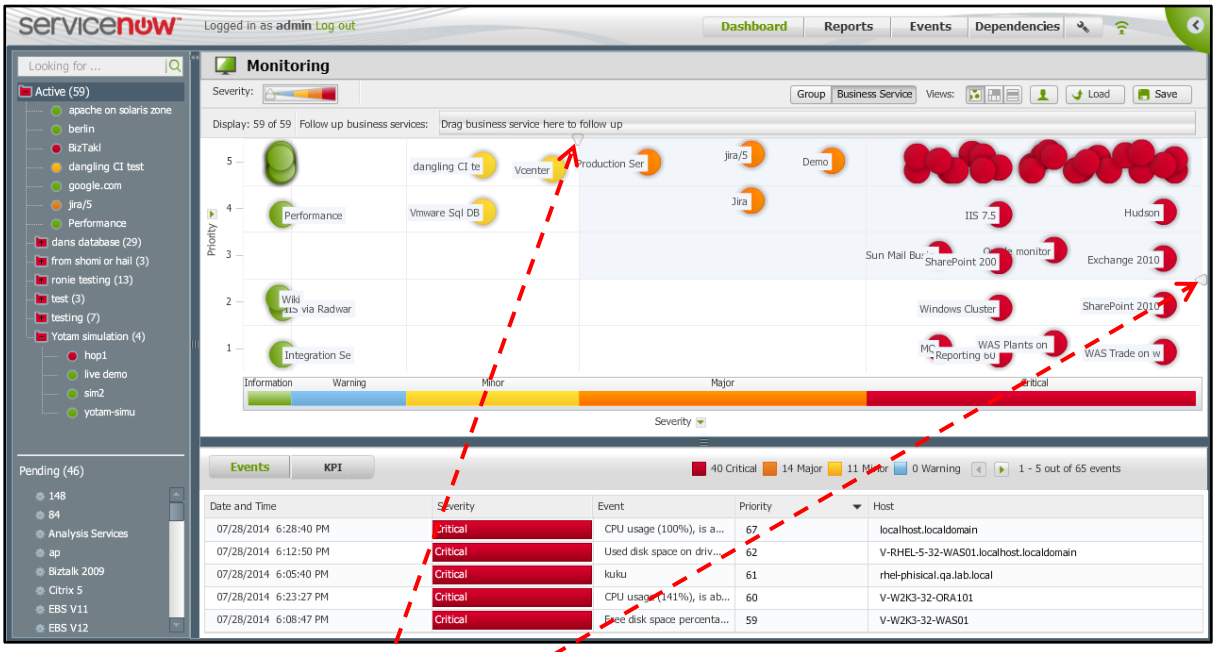
Bubble Format Dashboard

Figure 27 illustrates a dashboard whose **Monitoring** panel for **Active** business services displays each business service or group as a circle on a graph whose vertical axis is priority (or a user-defined metric such as revenue loss) and whose horizontal axis is severity.

Note: You can use the horizontal axis for a different user-defined measure but if you do, you lose the ability to display only business services whose severity is higher than the slider position.

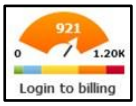
For each business service or group circle, a tool tip indicates its **name**, Priority, and Severity. For each business service circle, the tool tip has a link to its topology and a link to add it to the **Follow up business services** bar (analogous to a favorites list).

Figure 27: ServiceWatch Dashboard – Bubble format



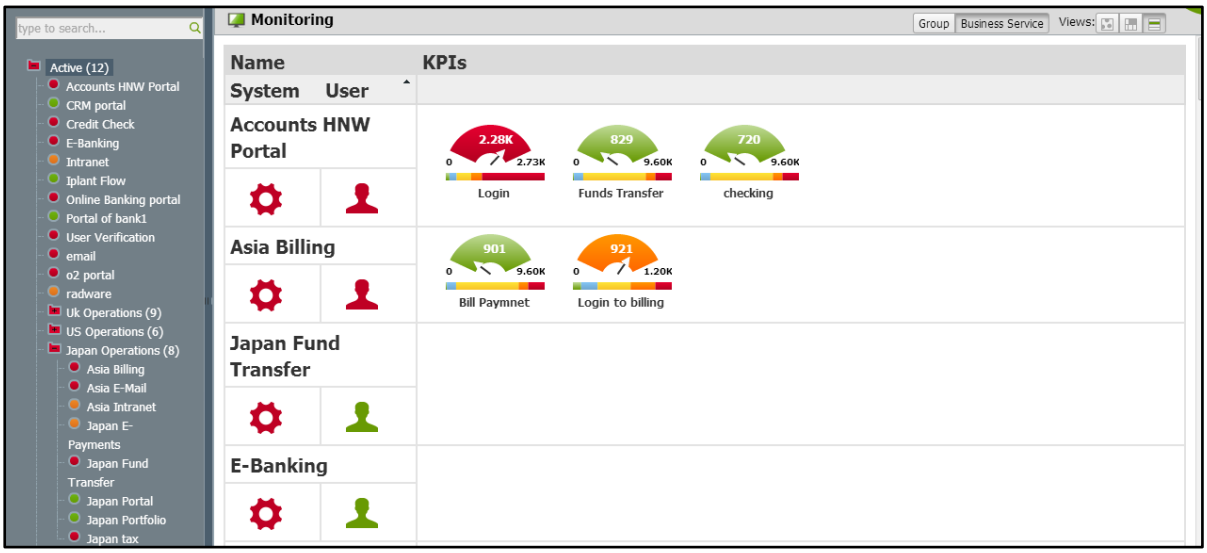
Arrows that slide along the top and right margins of the **Bubble** format change the configuration of the highlighted area. This helps visualize business services in that area as a group that requires attention. When the cursor hovers over an **Event** description, a tool tip displays the full description.

List Format Dashboard

Figure 28 illustrates the desktop/laptop List Format dashboard that displays each active business service and group on a horizontal row with  and  icons and with gauge 

icons for as many user-selected KPIs in each business service or group as will fit on its row.

Figure 28: ServiceWatch Dashboard – List format



The color of the  icon indicates the worst severity level of aggregate monitors, Synthetic monitors, and monitors dedicated to that business service or group (without regard to monitors at the CI level).

The color of the  icon indicates the worst severity level of any monitor associated with that business service or group (including monitors at CI level).

Note: CI level monitors are *not* displayed in the Standalone List Format because that format emphasizes the situation at the business service and group level and not at the CI level.

Gauge icons are displayed from left to right in alphabetical order for user-specified KPIs in each business service or group. There is no limit to the number of KPI gauges that a user can ask to display, but only as many gauge icons as will fit in the available horizontal space will be displayed.

The **KPI name** is displayed under each gauge icon.

The defined threshold bar for that KPI is displayed between the gauge and the **KPI name**. The numbers at each end of the threshold bar always range from low on the left to high on the right. End point numbers that can be theoretically exceeded are arbitrarily increased on the right (or decreased on the left) by 20%. Numbers followed by K should be multiplied by 1,000. Number followed by M should be multiplied by 1,000,000.

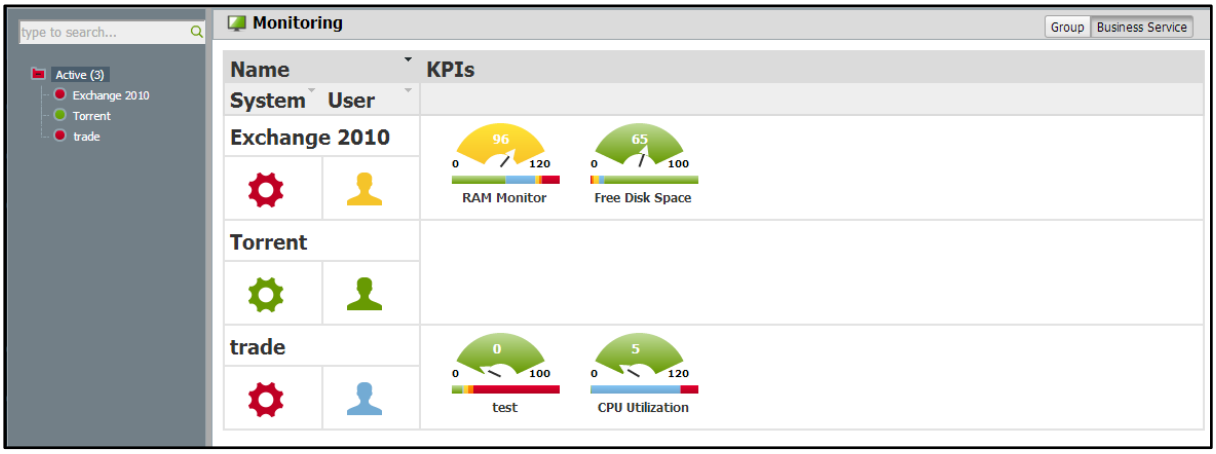
If Critical severities are associated with higher numbers, the red end of the threshold bar is on the right. If Critical severities are associated with lower numbers, the red end is on the left.

The color of the gauge indicates the current severity level of that KPI. The number in the gauge is the current value found by that monitor. The arrow in the gauge points to the relative location of that current value between the displayed low and high numbers.

Standalone List Format Dashboard

This format is designed for compatibility with a wide range of hand-held devices. In this format, only the **Monitoring** panel is displayed. The upper menu panel is not displayed because most hand-held devices do not support Flash which is required for displaying screens that can be displayed via that menu panel.

Figure 29: ServiceWatch Dashboard – List format in Standalone mode



Menu Bar Buttons

The **Menu** bar has 6 buttons, including a Collectors  icon plus a green area  in the top right corner that enables you to define a Business Service or Technical Business Service.

The currently active button name or Settings tool is **green**. The color of the  button indicates the status of the collectors. If you click this button, the System Health screen is displayed.

Figure 30: ServiceWatch Menu Bar buttons

Reports window

Click  to display the Reports window (see Figure 219: Reports window). This window contains a list of available Report Types and a list of automatically scheduled and manually generated Saved Reports. For information about this window and the Excel Reports Generator for producing custom reports, see CHAPTER 12: REPORTS.

Events window

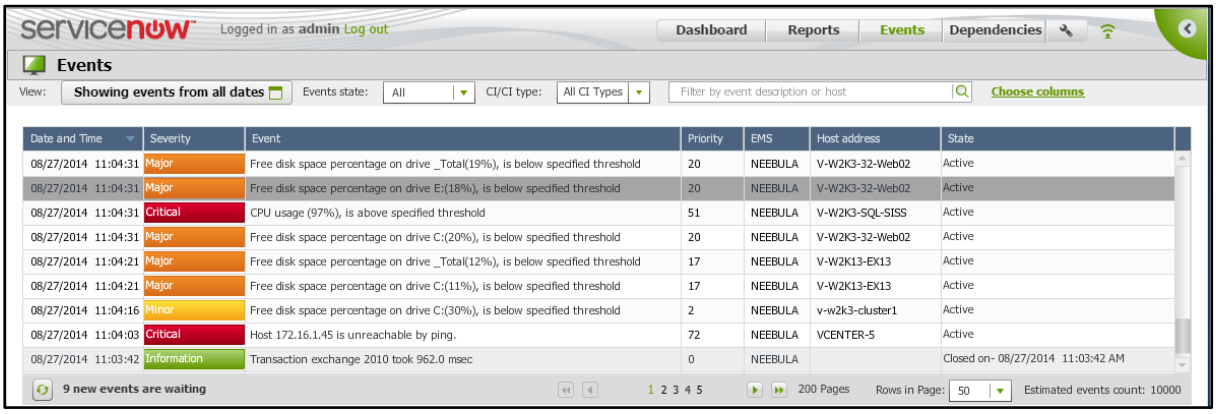
Click Events in the tool bar to display an **Events** window that contains a list of events. These events can be filtered by date range, event state (All, Active, Closed, Unbound), CI or CI type, and/or an Event Description or Host Name text string. See Chapter 7: Configuring Events for information about configuring events and integrating ServiceWatch with other event monitoring systems.

Click Choose columns to display the EMS Priority Host address checkboxes. Select or clear these checkboxes to display or hide the EMS, Priority and Host address columns in this window. After selecting the columns you want displayed, click Close.

For a description of the Event priority algorithm, see Event Priority on page 43.

Use this screen to find an event regardless of whether it is bound, active, or closed. You can close active events. An Events window is shown in Figure 31.

Figure 31: Events window

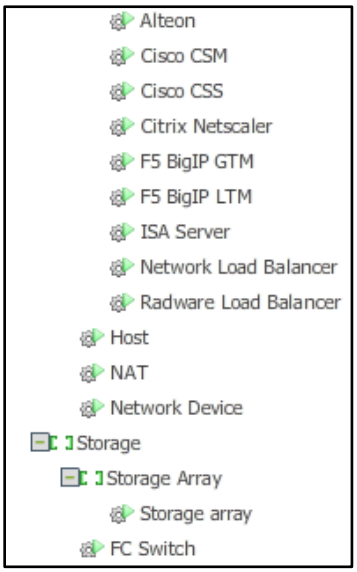


The default **View** range is **Show events from all dates**. To limit the display to a particular date/time range, click anywhere in the **View** box to display the **From/To** time range dialog box:

Click the **From/To** radio button, the calendar icons, and up and down hours:minutes arrows to specify or modify the **From – To** date/time range that filters the **Events** table. Click the **Events state** down-arrow to select a filter that displays **All**, **Active**, **Closed** or **Unbound** events.

Click the **CI/CI type** down-arrow to filter events by **CI name** or **type. CI types** are listed in Figure 32.

Figure 32: Typical CI Types



Type a string in the 

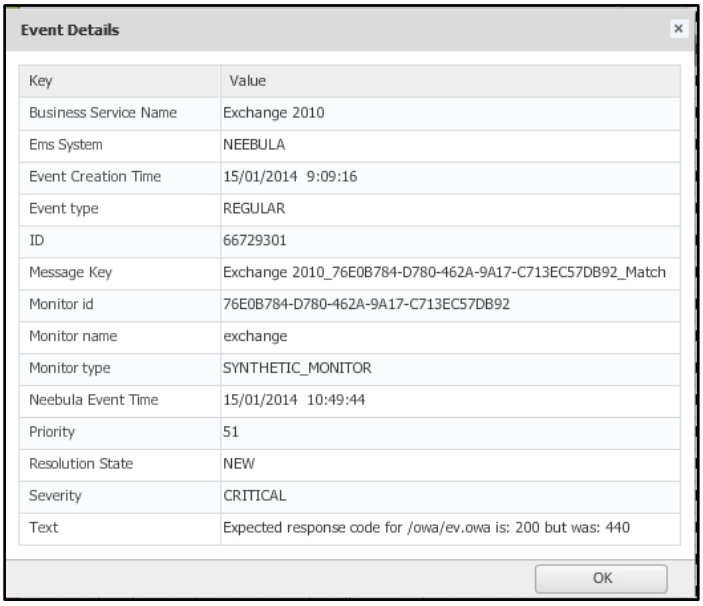
search field to limit the display to events that contain that string.

Click any column header to sort the window by that column. Click the same header again to reverse the sort order.

When the cursor hovers over an Event description, a tooltip displays the full text of that description.

Double-click anywhere on an event row to display its details in the **Event Details** window.

Figure 33: Event Details window



Click the **Key** or **Value** header to sort the window by that column. Click the same header again to reverse the sort order.

When the cursor hovers over a **Value**, the full text of that value is displayed in a tool tip.

Click 

or the  button to close the **Event Details** window.

For an alternative method of displaying Event details, see Displaying the details of an event in the Unbound Events Table on page 180.

Table 1 describes the Keys that may be listed in the **Event Details** window.

Table 1: Alphabetical list of Event Detail Keys

Key	Description
Business Service Name	Name of the business service affected by the event
Ems System	Name of the Event Management System that recorded the event
Event Creation Time	Date and time the event occurred
Event type	Type of event, e.g., REGULAR
Host Address	IP address of the host on which the event occurred
hwAddr	Hardware address of the device that generated or caused the event
ID	Unique event ID number
Message Key	A key generated by a binding rule that enables the record of an event to be located so that the event can be closed by a subsequent event
Monitor id	The unique ID number of the monitor that sensed the event
Monitor name	Name of the monitor that sensed the event
Monitor type	Type of monitor that sensed the event (business service, group, aggregated, synthetic)
Neebula Event Time	Date and time that Service Watch became aware of the event
Priority	See Event Priority on page 43 or page 182
Resolution State	State of the event (New, Unbound, Bound, Resolved)
Severity	Event severity level
Text	Text that describes the event
Unbound reason	Reason event was not bound to a CI, e.g., Event bound to host

Dependencies

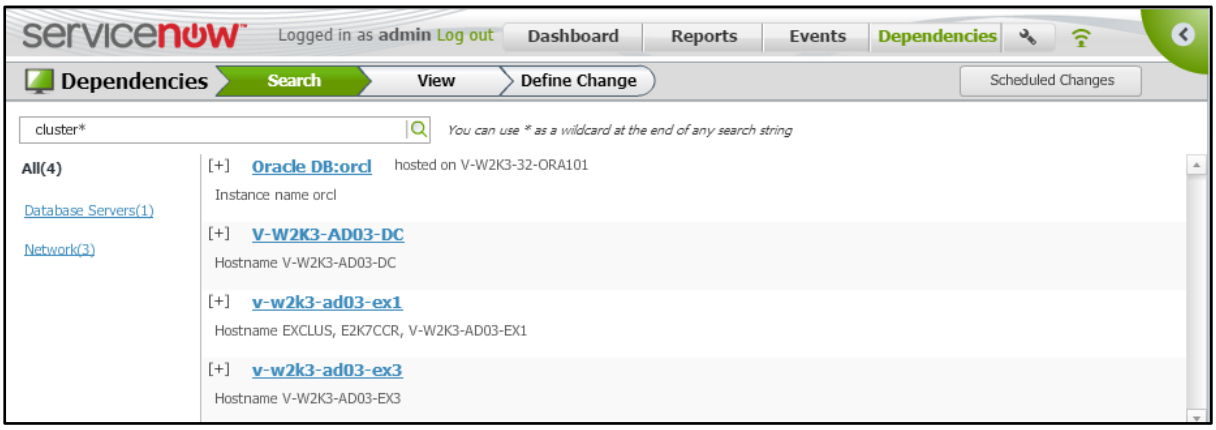
This feature enables you to search for a CI and then view its dependencies map and/or define changes to that CI.

Search for a CI

This screen finds CIs that match a search string without regard to business services they belong to.

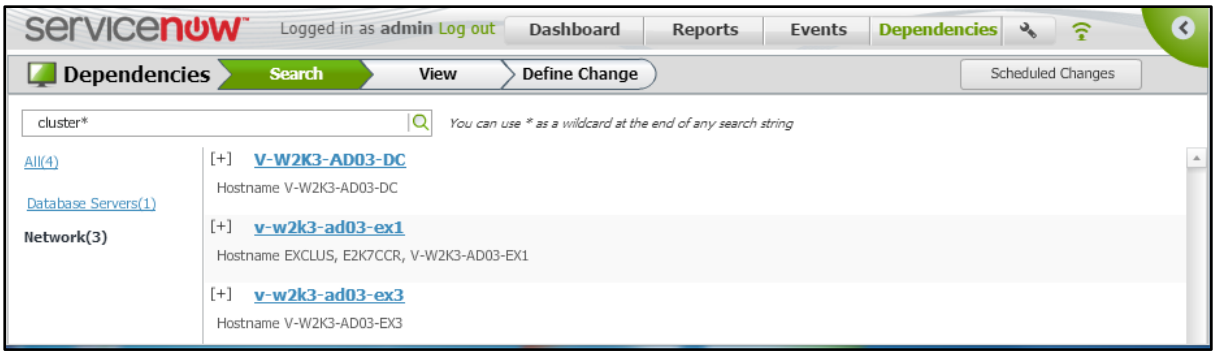
Click Dependencies and enter a search string. The string is *not* case sensitive. You can use ***** to represent any number of characters *at the end* of the string. While the cursor is in the search box, press the ↵ or **Enter** key to display all CIs that match the search string. The icon is *not* clickable.

Figure 34: Result of a Dependencies Search using a * wildcard



By default, all of the results are displayed in the main area of the Search panel. In the left pane, the matching CI Types are listed with the number (in parentheses) of each type found. Click a type **link** in the left column (e.g., **Network(3)**) to limit the display to results of that type.

Figure 35: Dependencies Search with results filtered

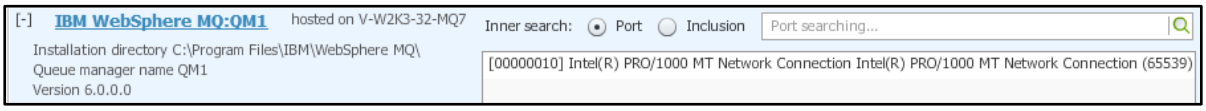


Inner Search

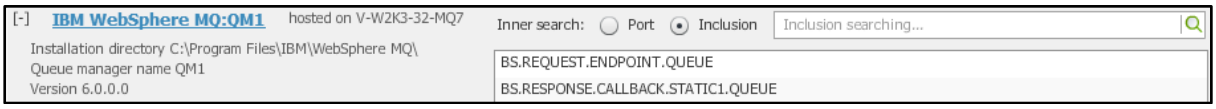
The 'inner search' enables you to find entities of the CI (e.g., ports, file system, volume, and inclusion data). These entities are CI-sensitive and only the relevant entities are displayed

Click the **[+]** on the row or anywhere on the row of a displayed CI *excluding its underlined link* to display a dialog box with radio buttons that enable you to display additional information about the selected CI. Click the **[-]** on a row to close its dialog box.

In this example, you can display **Port** data …



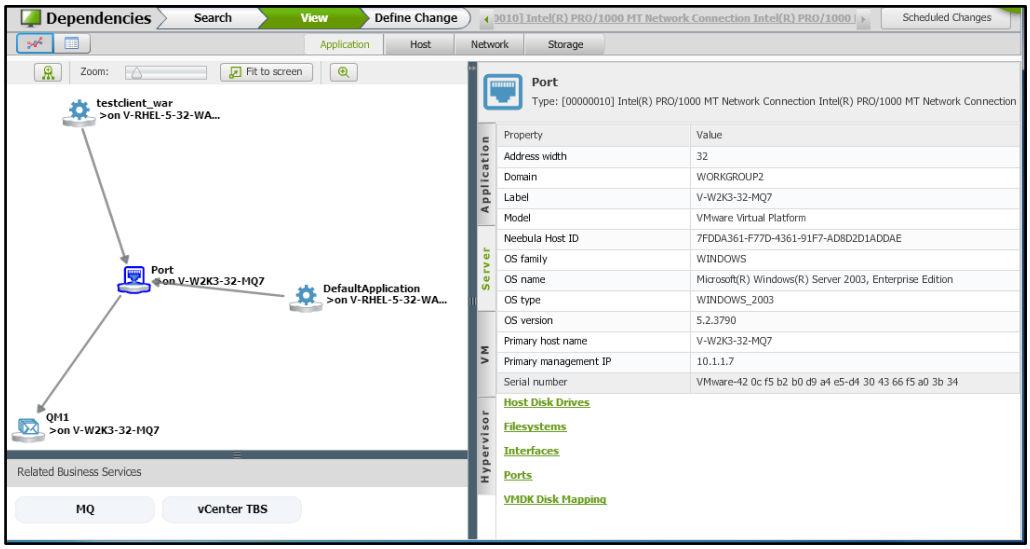
or **Inclusion** data. For other CIs, a **File system** or **Volume** radio button may be displayed.



- **Ports** are relevant for network & storage devices.
- **File systems** are relevant for hosts.
- **Volumes** are relevant for storage devices.
- **Inclusions** are relevant for CI parents of other CI types (e.g., EAR files for a WebSphere).

You can view more information about a specific entity by clicking its row in the **Port**, **Inclusion**, **Volume** or **File system** dialog box. For example, clicking the **Port** row displays the Topology map for that port:

Figure 36: Dependencies Search – Port Topology



Viewing CI information

Click a component link in the list of CIs to display its topology, location, and connectivity and its dialog box links in the **Application**, **Host**, **Network**, and **Storage panel**s.

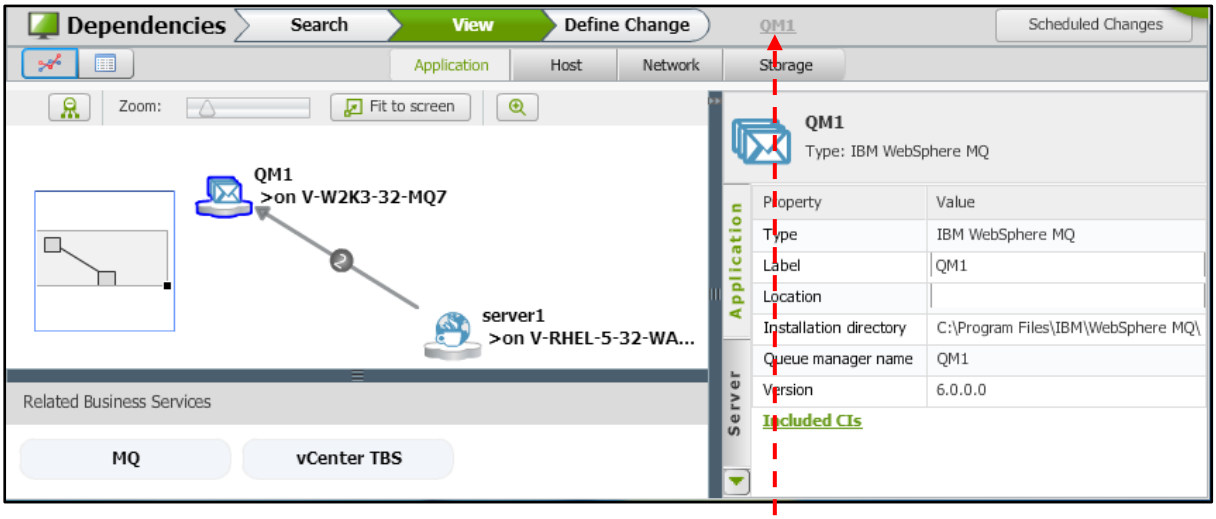
The Dependencies **View** window displays the CI or the CI's entity map of dependencies. It has 4 panels (**Application, Host, Network, Storage**). Each panel has 3 panes.

- The top left pane displays the topology (according to the selected tab).
- The bottom left pane displays its **Related Business Services**. Clicking a displayed Business Service will highlight the CIs that belong to it.
- The right pane displays properties of the CI selected in the topology.

The **Applications** panel displays Application, Server, VM & Hypervisor Property values plus links to relevant dialog boxes.

In this example, we clicked the link to IBM WebSphere MQ:QM1

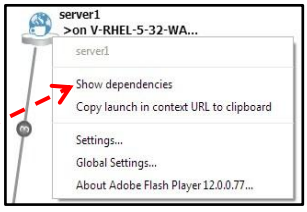
Figure 37: Dependencies window – Application panel



Navigating between CI views using Breadcrumbs

The CI name of the clicked component link is displayed as a 'breadcrumb' link in the top row of the **Dependencies** window. The currently displayed CI is grayed out.

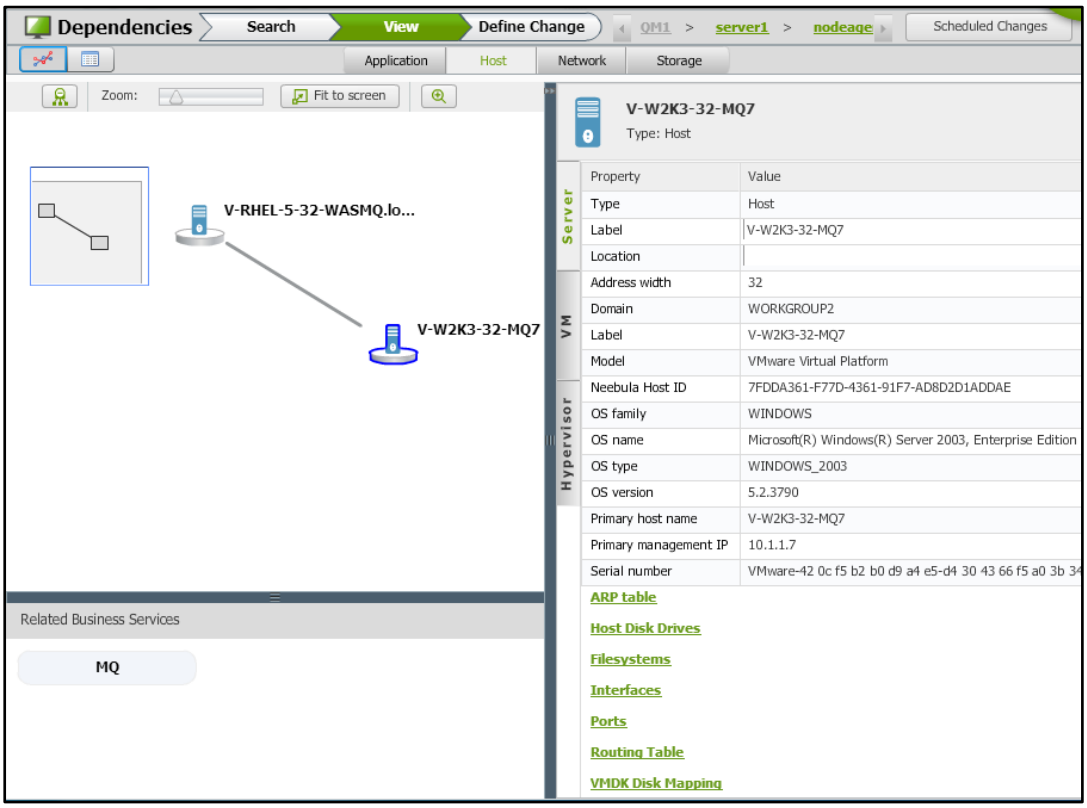
To view the dependencies of any CI that is currently displayed in this window, right-click that CI and select its **Show dependencies** option.



If breadcrumb links for previously displayed CIs do not fit in the top row, scroll-arrows will enable you to click previously displayed links.

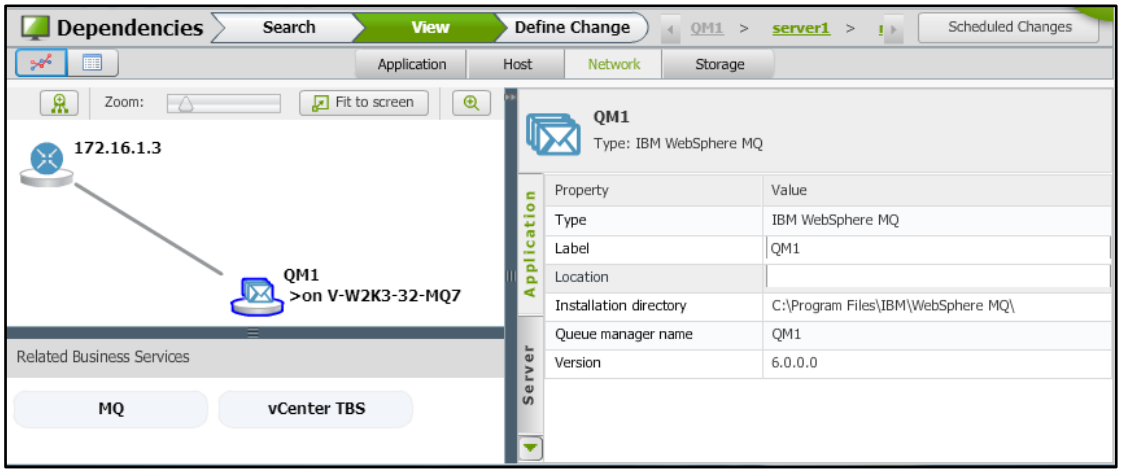
The **Host** panel displays Server, VM & Hypervisor Property values plus links to relevant dialog boxes.

Figure 38: Dependencies window – Host panel



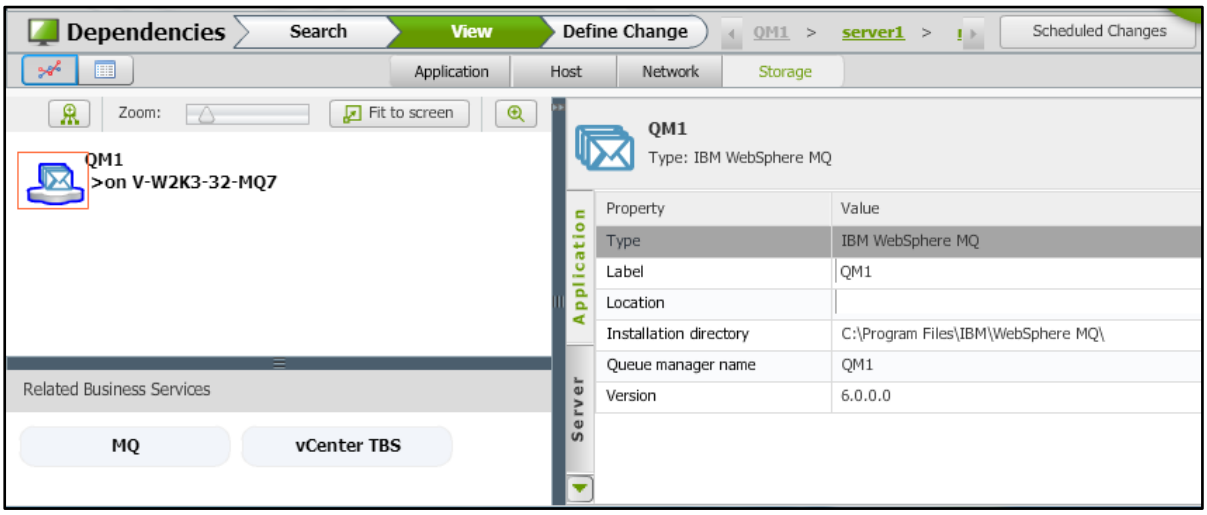
The **Network** panel displays Application, Server, VM and Hypervisor Property values (if any) plus links to relevant dialog boxes.

Figure 39: Dependencies window – Network panel



The **Storage** panel displays Property values and links to relevant dialog boxes.

Figure 40: Dependencies window – Storage panel



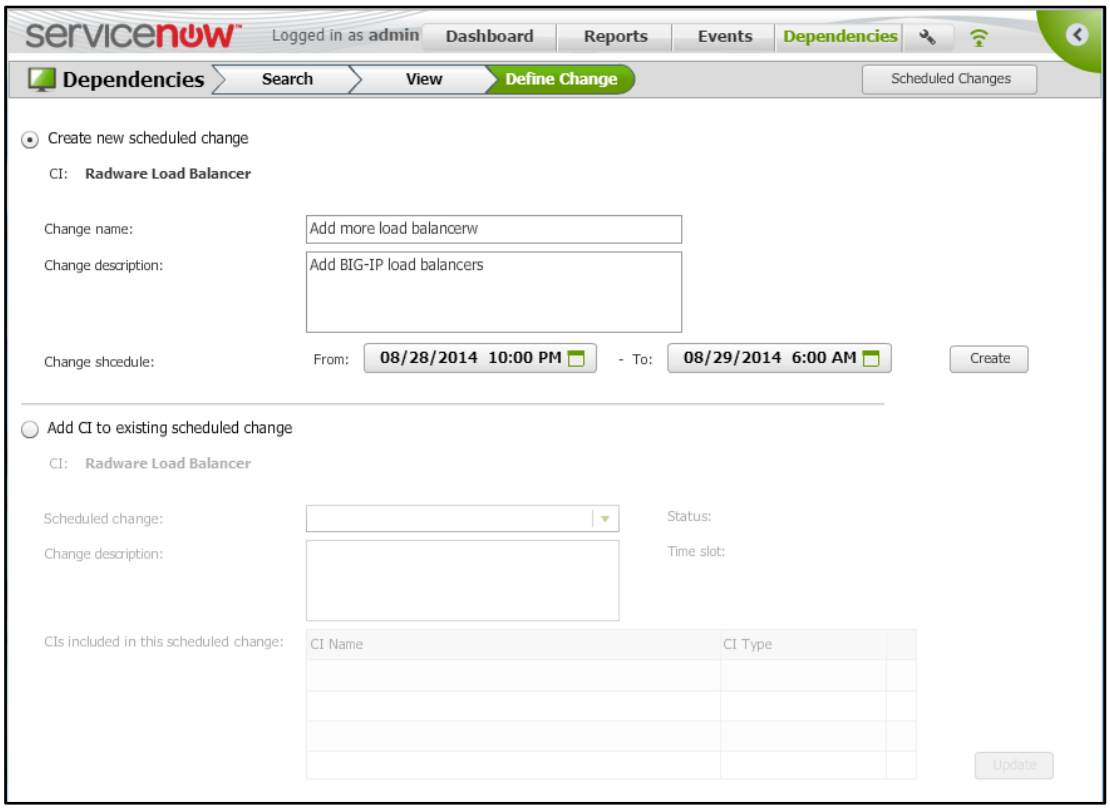
Define Changes to a CI

This feature enables you to define and schedule changes to a selected CI and to add a CI to a change that has already been defined and scheduled. The **Define Change** panel has two panes. Use the upper pane to define a new change. Use the lower pane to add a CI to an existing change.

Click the **Define Change** tab to display a panel whose radio buttons enable you to **Create** a **new scheduled change** for the currently displayed CI *or* to **add** that CI to an **existing scheduled change**.

Creating a new change

Figure 41: Define Change panel (create new change radio button selected)



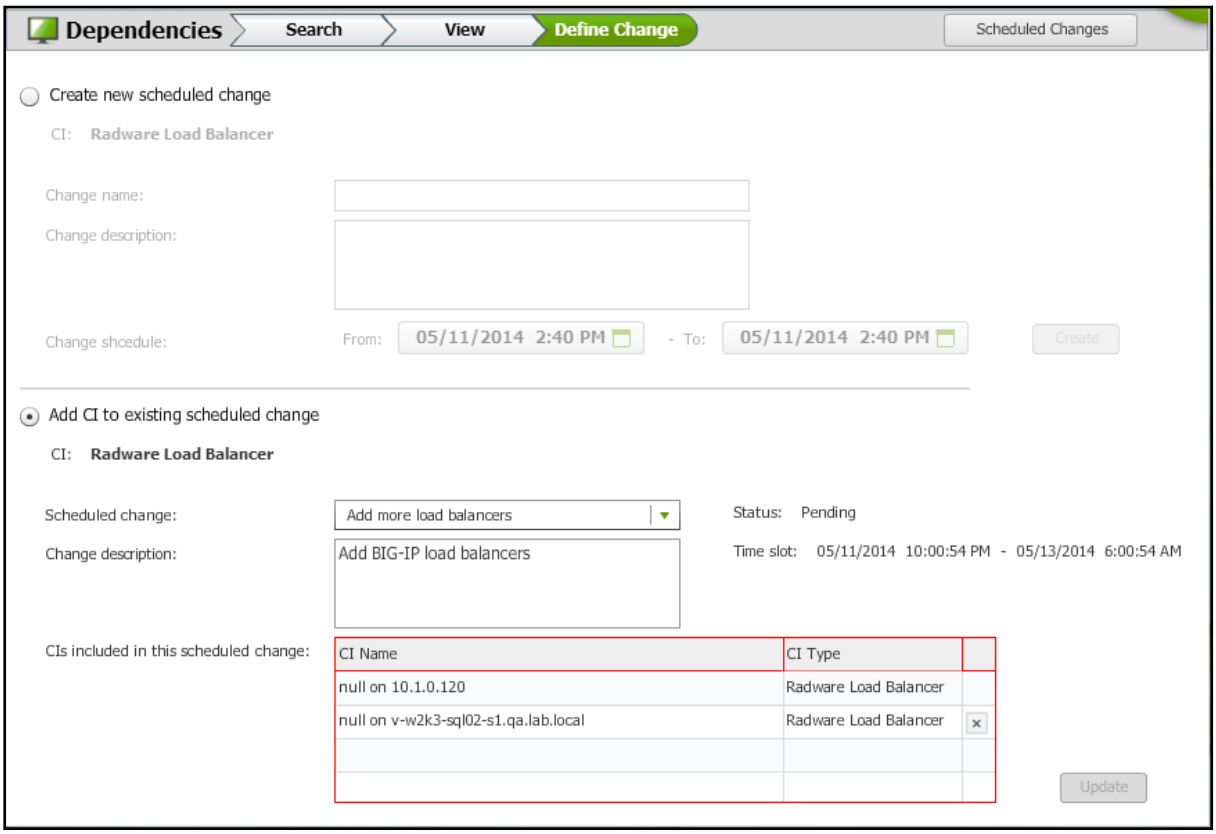
To define a new change that affects this CI, click the **Create new scheduled change** radio button, specify a meaningful **Change name** and type in a **Change description.** Schedule the change by specifying the **From – To** date range during which the change will take place, and click the **Create** button.

The Timeline Notes above Table 10 on page 203 describe how the history looks for CI removal or attribute changes that occur during a scheduled change interval. However, Topology changes during a scheduled change interval are displayed in the usual way.

The display of events that occur during a scheduled change interval is described under Figure 20 on page 43. Events occurring before and after the change interval are displayed in the usual way.

Adding a CI to an existing change

Figure 42: Define Change panel (add CI to existing change radio button)



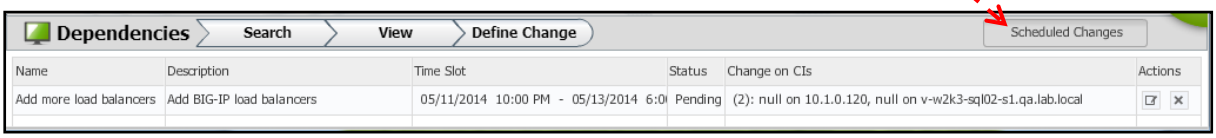
To add this CI to an existing scheduled change, click the **Add CI to existing scheduled change** radio button, click the **Scheduled change** down-arrow and select the existing **Scheduled change** from the drop-down list. The **Change description** for the selected change is displayed. Other CIs that have already been included in the selected change are listed in the table. Click the **Update** button to add the selected CI to the selected change.

In the bottom pane of this **Define Change** panel, the only modification that can be made to an existing change is to add a CI to it. However, the attributes of a change including its time frame can be modified by clicking its  button in the table of scheduled changes (see Figure 43 below).

Viewing all Scheduled Changes

To display all currently scheduled changes, click **the Scheduled Changes** button near the top right corner of the screen. A table of these changes is displayed.

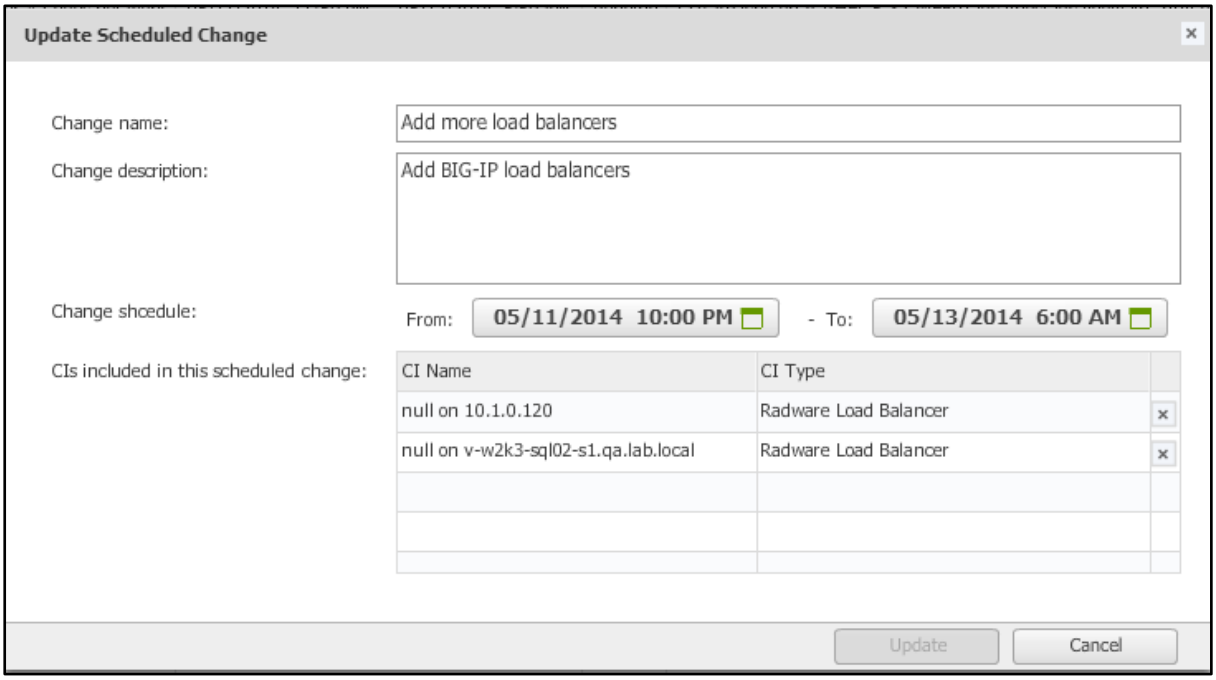
Figure 43: Dependencies window – Scheduled Changes table



Modifying a Scheduled Change

To edit a scheduled change, click its button or double-click its row in the table of Scheduled Changes. The **Update Scheduled Change** dialog box is displayed. In this dialog box, CIs can be deleted and the time frame can be updated.

Figure 44: Update Scheduled Change dialog box



Make the desired changes in this dialog box and click the **Update** button.

Host View

The **Host view** icon  in the Topology Map panel toggles between the default display of CIs & hosts or the display of *only* hosts in **Host view** mode. The Host view can help determine that all of the hosts were discovered and help locate connections to each host.

Figure 45: Topology Map with CIs and Hosts displayed

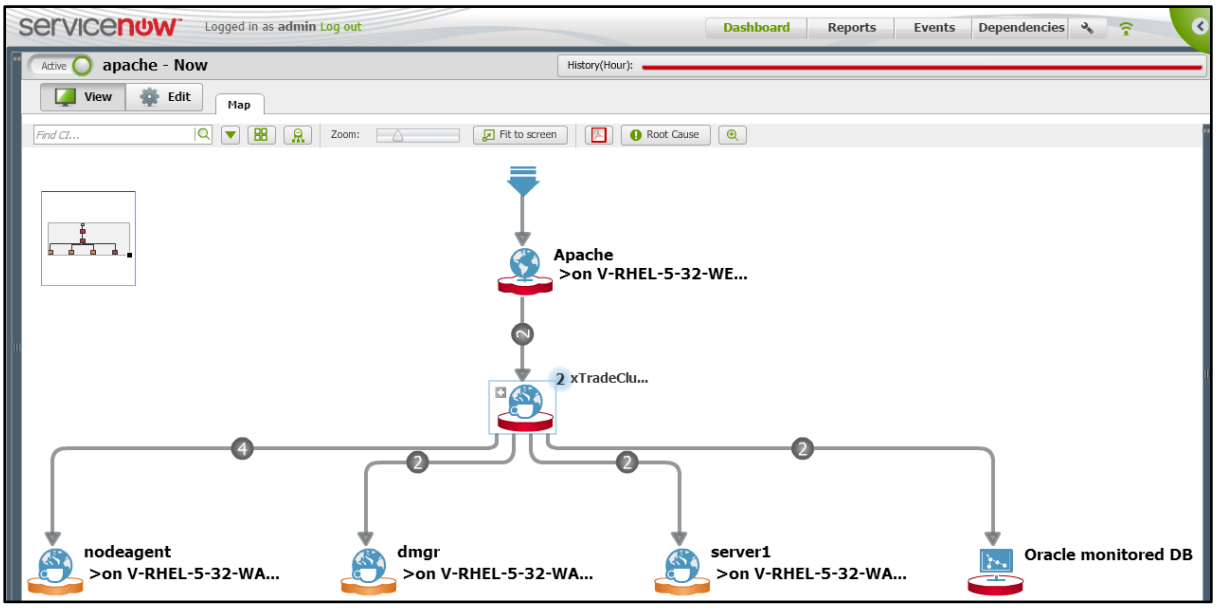
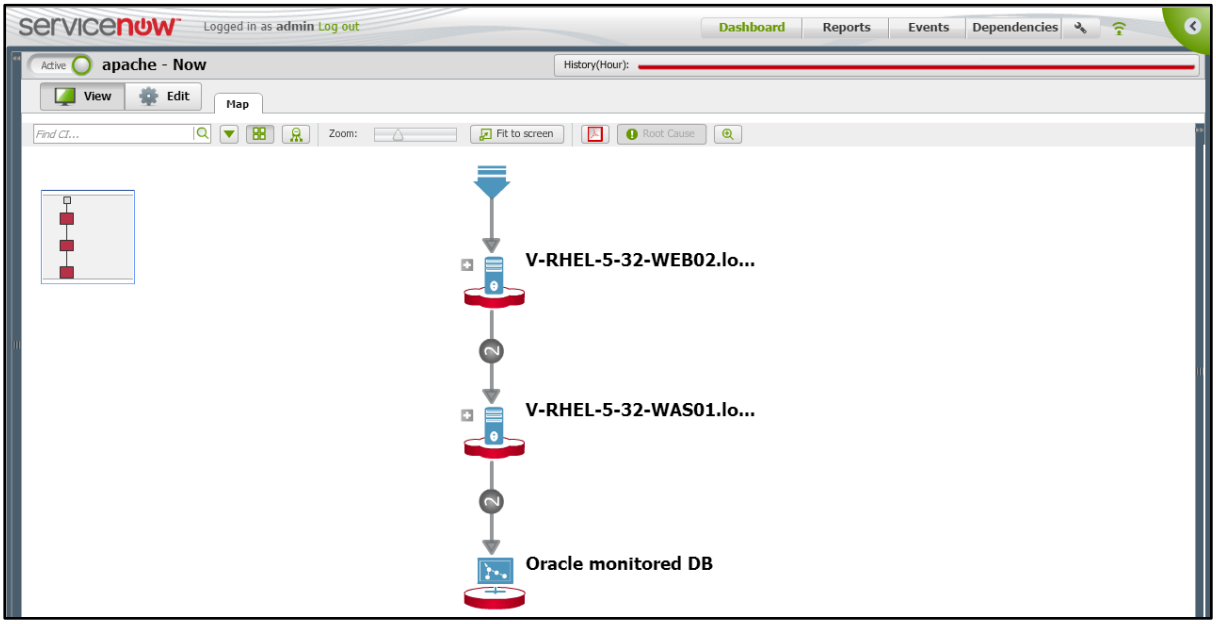


Figure 46: Topology Map with only Hosts displayed



System Health

The System Health button is **green** if all of the Collectors are active. Otherwise, the button is **red**. To display the **System Health** screen, click , or click and select the **System Health** option in the **Settings** menu. The color of the icon in each panel tab indicates the worst severity of any system element associated with that tab.
By default, the most recently used panel is displayed.

Server Status panel

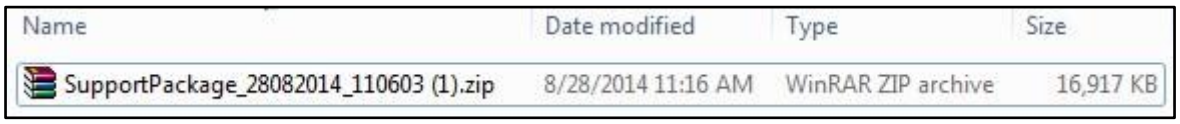
The **Server Status** panel contains information about the health of the relevant server and buttons to create a support package and to produce an audit log.

Figure 47: System Health screen – Server Status panel

The ServiceWatch Customer Support team may ask you to send them a **Support Package** that contains information about your system to help them solve a problem. To create this **Support Package**, click the Create Support Package button. After the Support Package is created, you will receive a message similar to:

Download link for the support package: http://10.1.1.29:8080/static/support/SupportPackage_28082014_110603.zip

Store the **Support Package** in a location accessible to ServiceWatch Customer Support or send it to them attached to an email. A typical **Support Package** has these attributes:



To view the **Audit Log**, click the Get Audit Log button. A link similar to this one will be displayed:

Download link for the audit log package: http://10.1.1.29:8080/static/support/audit_log.zip

When you click this link, a Windows dialog box enables you to Open, Save, or rename and designate a location to save the **Audit Log**. Customer Support may also request a copy of this **Audit Log**.

A typical **Audit Log** may have the following characteristics:

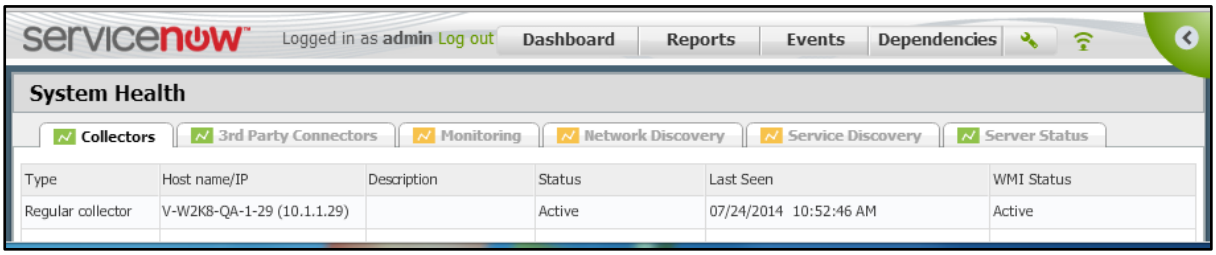
Name	Type	Compressed size	Password protected	Size	Ratio	Date modified
audit.log	Text Document	1 KB	No	8 KB	89%	3/11/2014 4:48 PM

Collectors panel

Click the **Collectors** tab to display the health status of each ServiceWatch Collector. The color of the icon in this tab indicates the worst severity of any Collector displayed in the panel.

Click any column header to sort the data in this panel by that column.
Click the same header again to reverse the sort order.

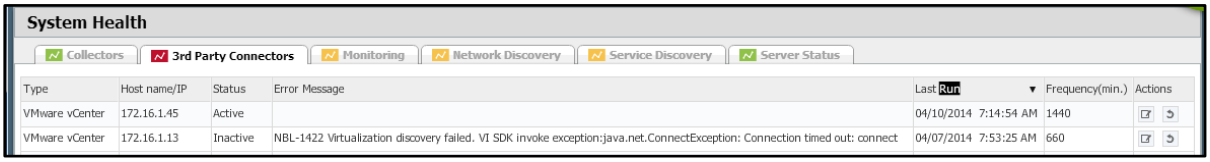
Figure 48: System Health screen – Collectors panel



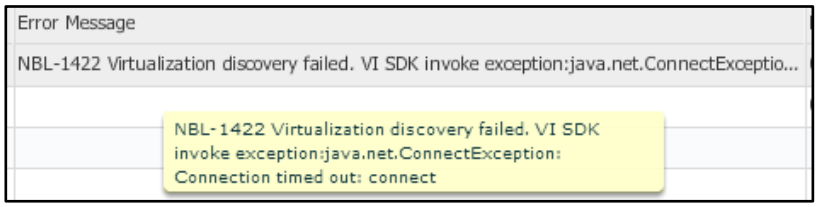
3rd Party Connectors panel

This panel displays the health status of each 3rd Party Connector. Click the **3rd Party Connectors** tab to display this panel. Click any column header (except **Actions**) to sort the data in this panel by that column. Click the same header again to reverse the sort order.

Figure 49: System Health screen – 3rd Party Connectors panel



If an error message is not completely displayed, hold the cursor over that message to display all of it in a tool tip.



Actions column

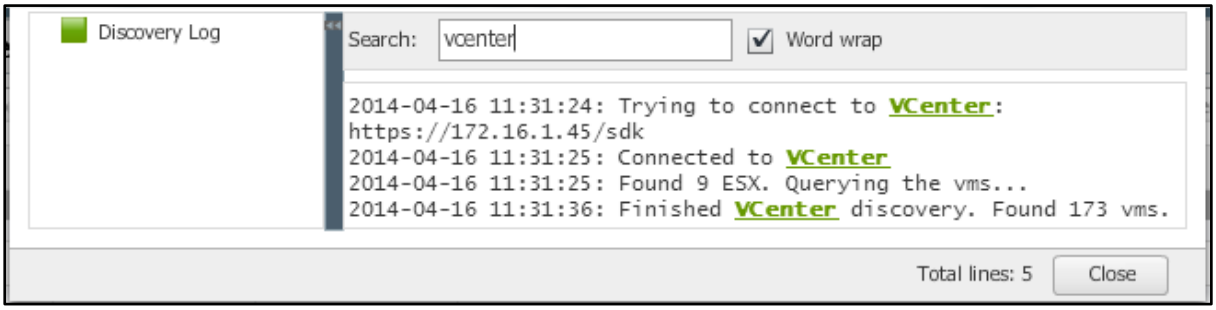
The **Actions** column contains a **Show discovery log** button and a **Reconnect** button. If you click , a **Reconnect 3rd Party Connector** message is displayed.

Click the **Show discovery log** button to display the log contents. The log contains a trace of all 3rd party connector activity and is used by ServiceWatch Customer Support to diagnose problems.

If you type a (case irrelevant) string in the **Search** box, instances of that string will be bolded, underlined and displayed in green.

If the **Word wrap** checkbox is selected, text that is too long to fit on a line will be displayed on the next line instead of being truncated.

Figure 50: 3rd Party Connectors – Discovery Log window

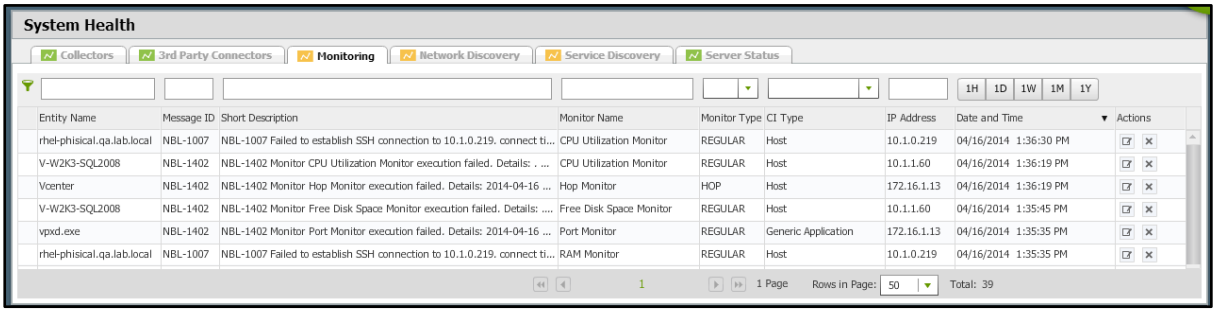


Click Close to close the **Discovery Log** window.

Monitoring panel

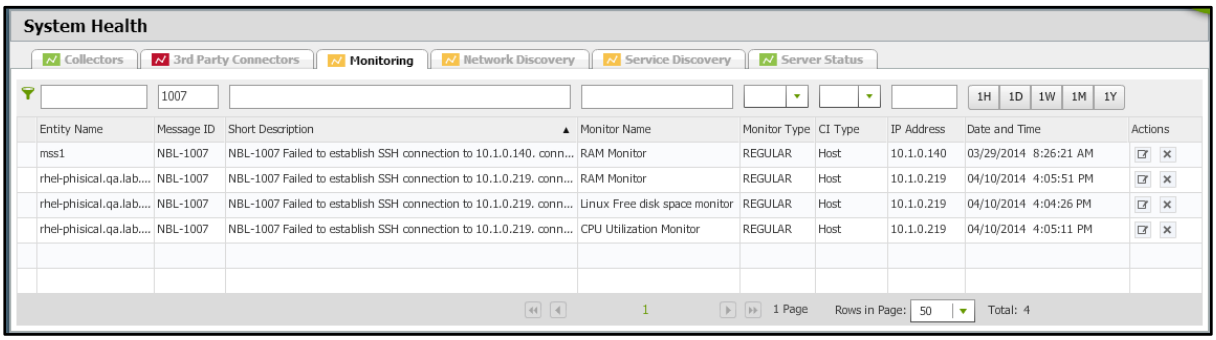
This panel displays the health status and messages associated with ServiceWatch monitors. Click the **Monitoring** tab to display this panel. Click any column header (except **Actions**) to sort the data by that column. Click the same header again to reverse the sort order.

Figure 51: System Health screen – Monitoring panel



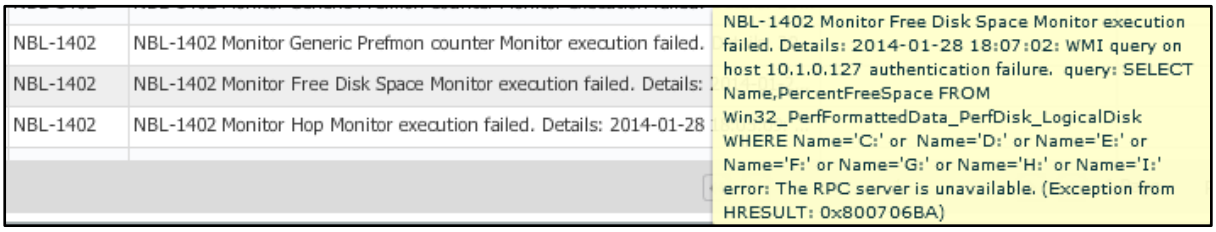
To filter messages by **Entity Name**, **Message ID**, **Short Description**, **Monitor Name** or **IP Address**, enter a text string in the text box above these columns. There are no wildcards. Records are displayed if the trimmed search string occurs anywhere in the field. Click **Enter** or ↵ to display only data that matches that string. For example, to display only messages whose **Message ID** contains 1007:

Figure 52: System Health screen – Monitoring panel filtered by Message ID

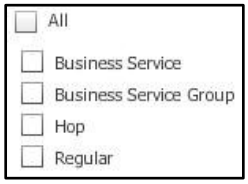


If the cursor hovers over a **Short Description** text, the full description is displayed in a tooltip. For example:

Figure 53: Full Description in a tool tip



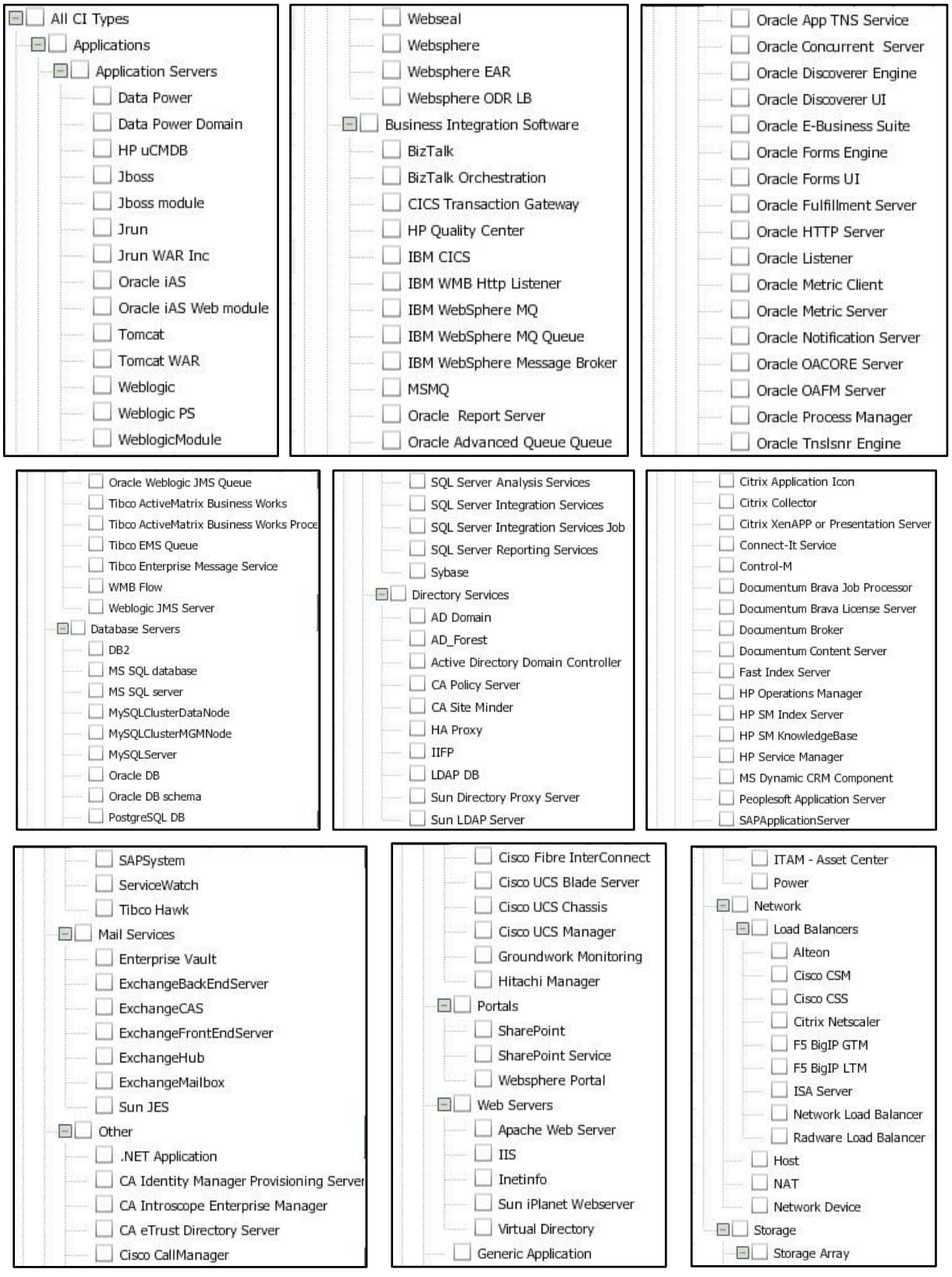
To filter messages by **Monitor Type**, click the down-arrow above the header and select the desired options in the drop-down menu.



Click one of the 1H 1D 1W 1M 1Y buttons to limit the display to messages generated during the last hour, day, week, month or year.

To filter messages by **CI Type**, click the down-arrow above the header and select the desired nodes in the drop-down tree. Nodes in the CI Type tree can be expanded and collapsed.

Figure 54: Expanded CI Type nodes



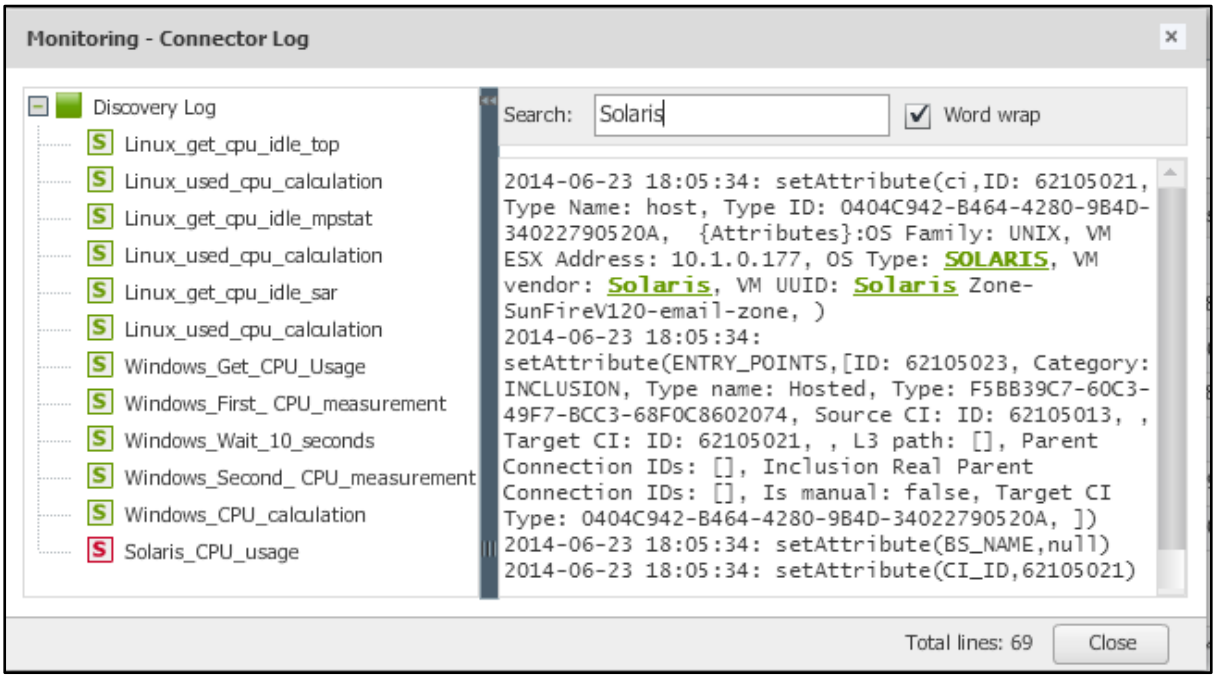
Actions column

The **Actions** column contains a **Show discovery log** button and a **Reconnect** button. If you click the button on a message row, the **Discovery Log** for that message is displayed. The **Discovery Log** node in the left panel may have subnodes that are appropriate to the message.

If you type a (case irrelevant) string in the **Search** box, instances of that string will be bolded, underlined and displayed in green.

If the **Word wrap** checkbox is selected, text that is too long to fit on a line will be displayed on the next line instead of being truncated.

Figure 55: Monitoring panel Discovery Log

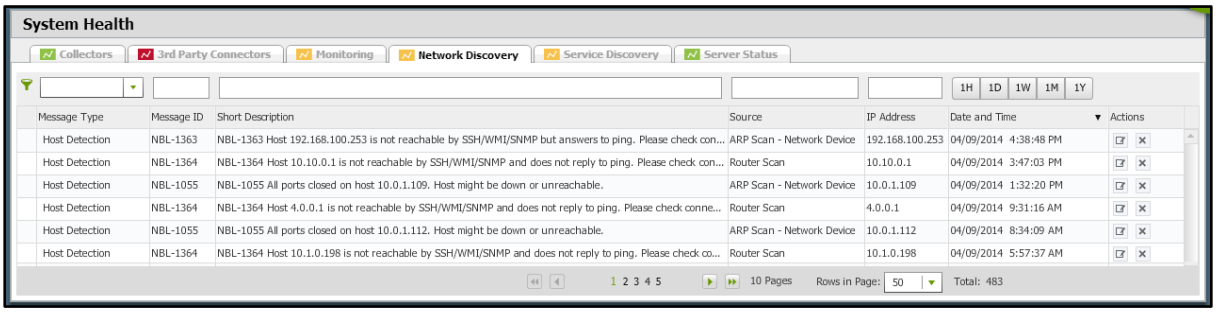


If you click the button, that log entry is deleted.

Network Discovery panel

This panel displays messages that were generated automatically by the system. On the other hand, messages in the **Service Discovery** panel are generated as a result of user actions. Click the **Network Discovery** tab to display this panel. Click any column header (except **Actions**) to sort the data in this panel by that column. Click the same header again to reverse the sort order.

Figure 56: System Health screen – Network Discovery panel



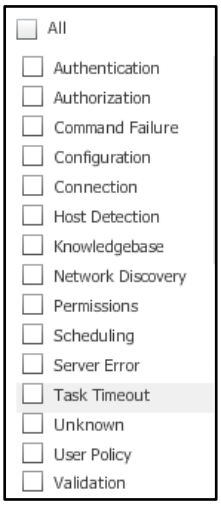
Type a string in any of the text boxes above each column and click **Enter** or ↵ to display only data that matches that string. There are no wildcards. Records are displayed if the trimmed search string occurs anywhere in the field. For example, to display only messages whose **Message ID** contains 1005:

Figure 57: System Health screen – Network Discovery panel filtered by Message ID

Click one of the 

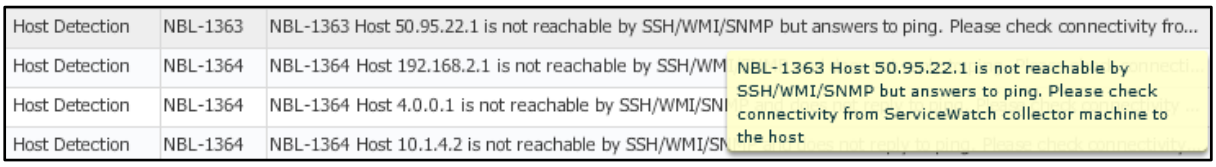
buttons to limit the display to messages generated during the last hour, day, week, month or year.

To filter messages by message type, click the down-arrow above the **Message Type** header, select desired types from the drop-down list, and close the list.



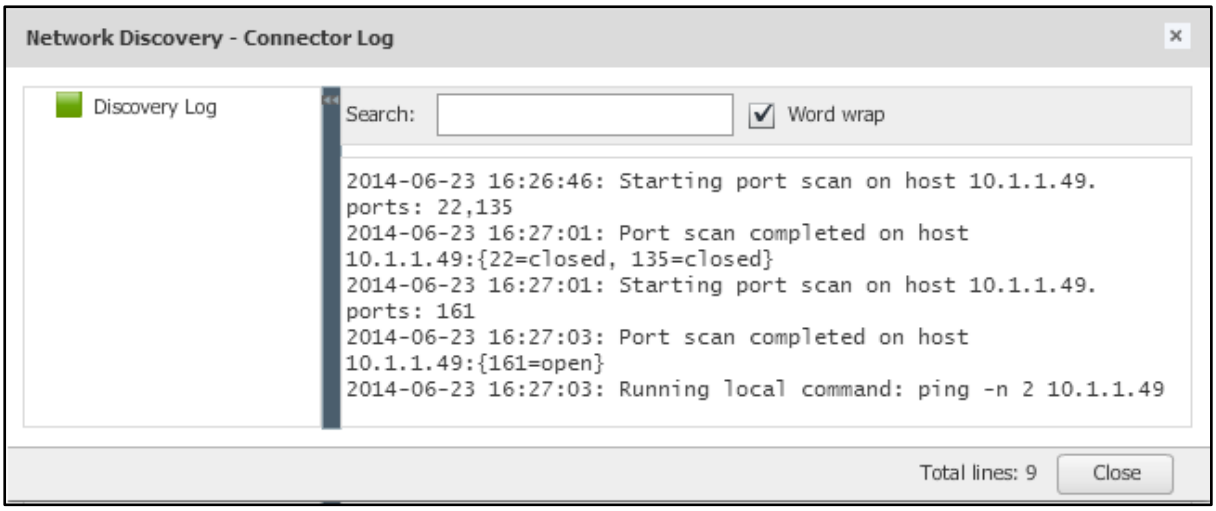
If the cursor hovers over a **Short Description** text, the full description is displayed in a tooltip. For example:

Figure 58: Full Description in a tool tip



The **Actions** column contains a **Show discovery log** button and a **Delete** button. If you click the button on a message row, the **Discovery Log** for that message is displayed.

Figure 59: Network Discovery Log



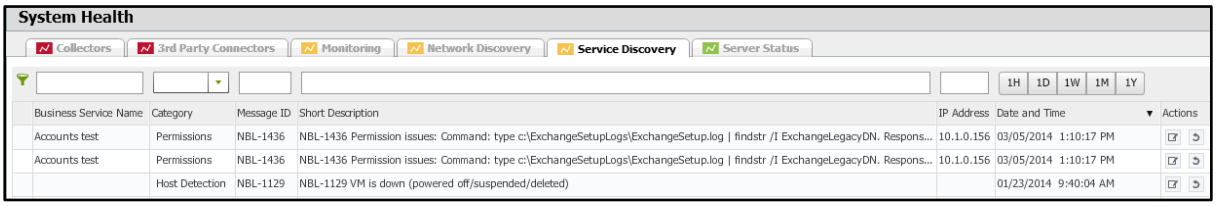
If you type a (case irrelevant) string in the **Search** box, instances of that string will be bolded, underlined and displayed in green.

If the **Word wrap** checkbox is selected, text that is too long to fit on a line will be displayed on the next line instead of being truncated.

Service Discovery panel

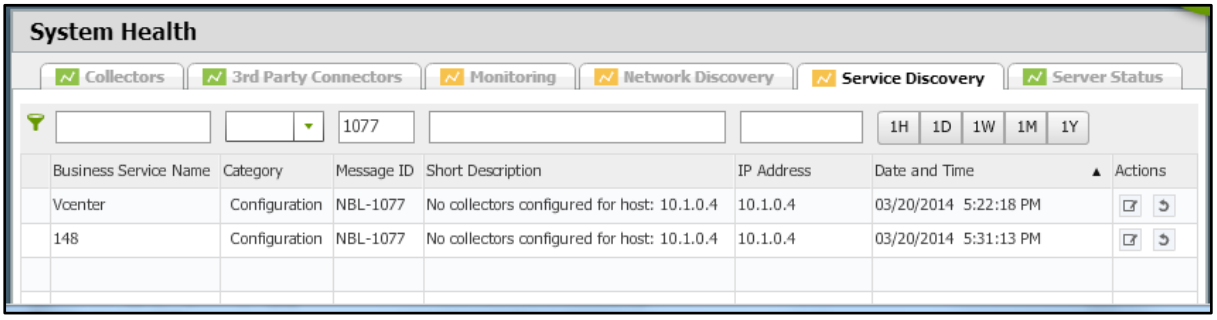
This panel displays messages that were generated as a result of top down business service discovery initiated by the user. On the other hand, messages in the **Network Discovery** panel are generated automatically by the system. Click the **Service Discovery** tab to display this panel. Click any column header (except **Actions**) to sort the data in this panel by that column. Click the same header again to reverse the sort order.

Figure 60: System Health screen – Service Discovery panel



Type a string in any of the text boxes above each column and click **Enter** or ↵ to display only data that matches that string. There are no wildcards. Records are displayed if the trimmed search string occurs anywhere in the field. For example, to display only messages whose **Message ID** contains 1077:

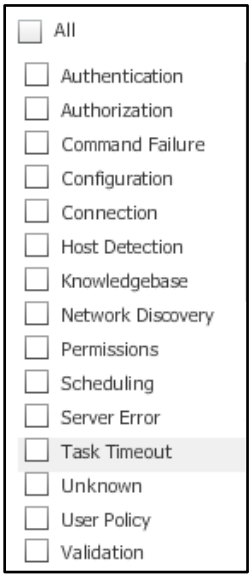
Figure 61: System Health screen – Service Discovery panel filtered by Message ID



Click one of the 

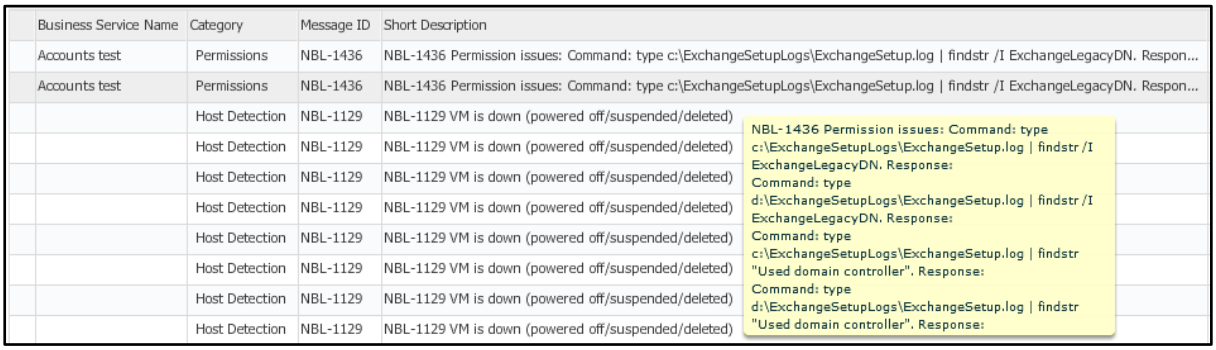
buttons to limit the display to messages generated during the last hour, day, week, month or year.

To filter messages by **Category**, click the down-arrow above the heading and select the desired message types from the drop-down menu.



If the cursor hovers over a **Short Description**, a full description is displayed in a tooltip.

Figure 62: Full Description in a tool tip

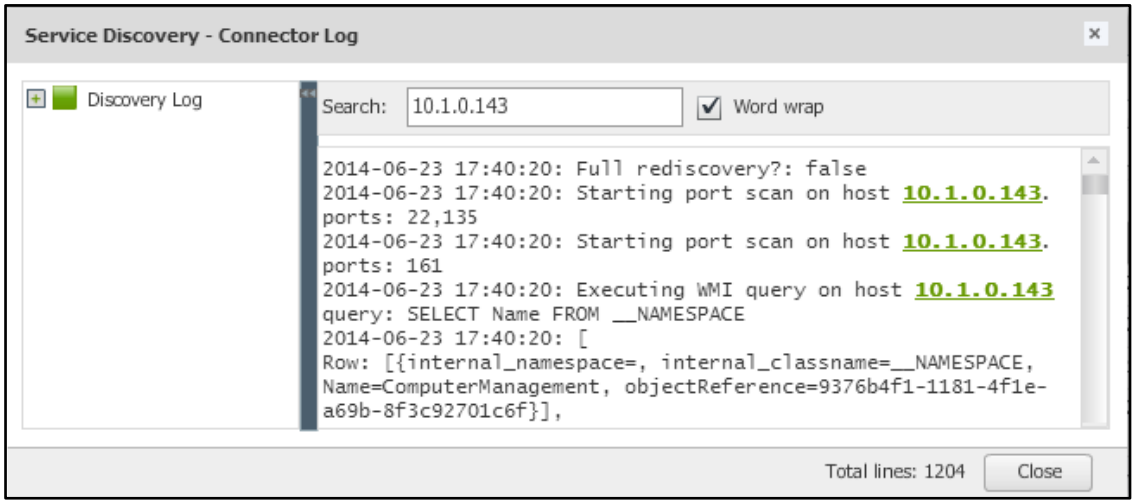


Actions column

The **Actions** column contains a **Show discovery log** button and a **Resume Discovery** button. If you click , a **Resume Discovery** message is displayed.

Click the **Show discovery log** button to display the log contents. The log contains a trace of all Business Service discovery activity and is used by ServiceWatch Customer Support to diagnose problems. If you type a (case irrelevant) string in the **Search** box, instances of that string will be bolded, underlined and displayed in **green**.

Figure 63: Business Service Discovery screen – Discovery Log window



The **Discovery Log** node in the left panel may have subnodes that are appropriate to the message.

Click Close to close the **Discovery Log** window.

If you type a (case irrelevant) string in the **Search** box, instances of that string will be bolded, underlined and displayed in **green**.

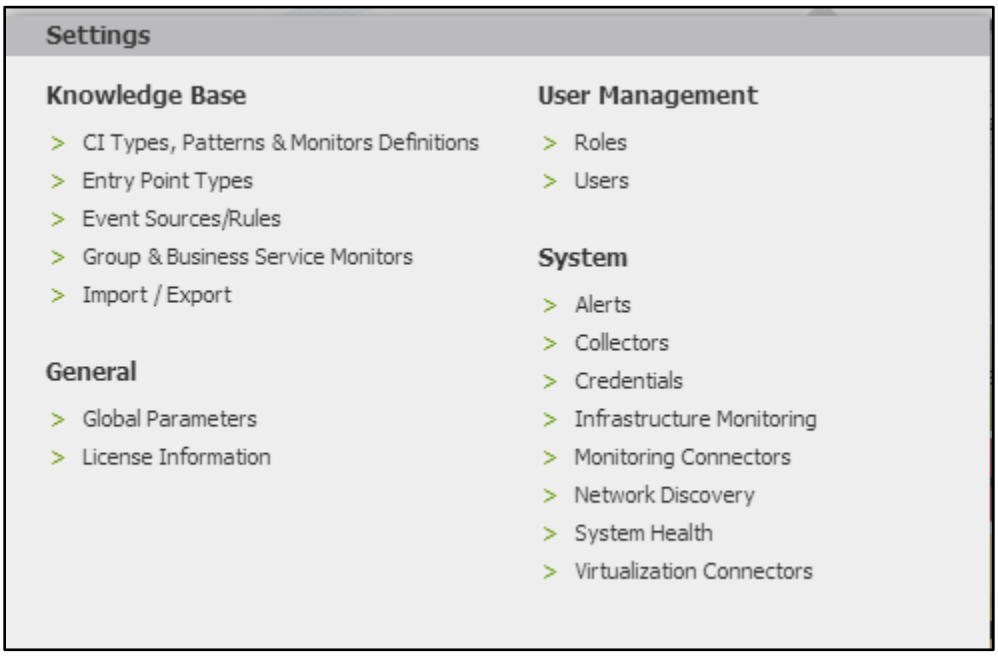
If the **Word wrap** checkbox is selected, text that is too long to fit on a line will be displayed on the next line instead of being truncated.

Chapter 5: Settings

Settings Menu

Clicking the  icon displays the **Settings** menu with links to each **Settings** option.

Figure 64: Settings menu



Parameter Types

Knowledge Base

- CI Types, Patterns & Monitors Definitions – Define attributes of a Configuration Item (CI) Type (page 74).
- Entry Point Types – Duplicate or clone a node in the left panel (page 83).
- Event Sources/Rules – Define rules that bind events or groups of events to CIs or hosts (page 85).
- Group & Business Service Monitors – Create, delete, modify business service monitors (page 86).
- Import / Export – Import or export all of the Knowledge Base or selected CI Types (page 89).

General settings

- Global Parameters – Modify default values of some ServiceWatch system parameters (page 93).
- License Information – Display number of business service hosts that were discovered (page 105).

User Management setting

- Roles – Create & define roles and the permissions & responsibilities assigned to each (page 106).
- Users – Define system users after defining the roles that will be assigned to them (page 109).

System

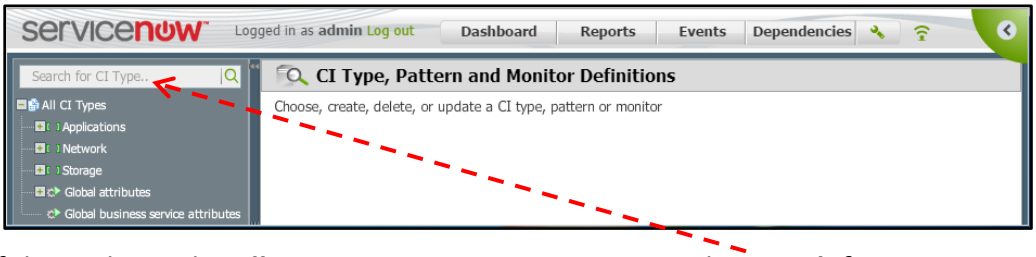
- Alerts – Specify notification triggers for changes & status changes in business services (page 111).
- Collectors – Define and limit the IP ranges of collectors (page 114).
- Credentials – Enables the discovery of configuration items in your network (page 116).
- Infrastructure Monitoring – Schedule and activate ServiceWatch-built and home-built infrastructure monitors for network devices and storage arrays (page 121).
- Monitoring Connectors – Specify parameters for gathering events from 3rd party connectors such as HP Overview, Netcool, MOM and SolarWinds (page 122).
- Network Discovery – These parameters determine whether and how often discovery should be performed and which IP ranges should be excluded from the process (128).
- System Health – Display discovery messages about Collectors, 3rd Party Connectors, Monitoring, Network Discovery, Service Discovery and Server Status (page 63).
- Virtualization Connectors – Specify parameters for discovery via virtualization vendors such as Amazon AWS, EMC ECC, VMware vCenter, and Citrix XEN (page 128).

Knowledge Base settings

CI Types, Patterns & Monitors Definitions

Click the **CI Types, Patterns & Monitors Definitions** link in the **Settings** menu (Figure 64) to display the **CI Type, Pattern and Monitor Definitions** window. Select a CI type or pattern (Figure 65) in the **All CI Types** tree to modify its definition *or* right-click an entity in that tree and select a right-click menu option for that entity.

Figure 65: CI Type, Pattern and Monitor Definitions window



To expand *all* of the nodes in the **All CI Types** tree, type one space in the **Search for CI Type** search box.

Table 2: Alphabetical list of Entity Types

Entity Type	Entity Type
Applications	Mail Services
AD Domain Controller	MS SQL database
Apache Web Server	MS SQL server
Application Servers	MySQLClusterDataNode
Billing	MySQLClusterMGMNode
Business Integration Software	MySQLServer
CA Identity Mgr Provisioning Server	NAT
CA Introscope Enterprise Manager	.NET Application
CA eTrust Directory Server	Network
Cisco CallManager	Network Device
Cisco Fabric Interconnect	Oracle DB
Cisco UCS Blade Server	Oracle DB schema
Cisco UCS Chassis	Other
Cisco UCS Manager	PC Switch
CPU Utilization Monitor	Ping monitor
Database Servers	Port Monitor
DB2	Portals
Directory Services	PostgreSQL DB
Domain Ctrl. on Windows	RAM Monitor
Enterprise Applications	SharePoint
Free Disk Space Monitor	SharePoint Service
Generic Application	SQL Server Analysis Services
Generic Applications CI	SQL Server Integration Services
Global attributes	SQL Server Integration Services Job
Global business service attributes	SQL Server Reporting Services
Host	Storage
IBM CICS	Storage Array
IIFP	Sun iPlanet Webserver
IIS	SWAP Monitor
Inetinfo	Sybase
ITAM – Asset Center	TCP Monitor
LDAP Database	Virtual Directory
Linux Free Disk Space Monitor	Web Servers
Load Average	WebSphere Portal
Load Balancers	

Right-click menu options for CI Type categories, CI Type entities and CIs

The only right-click menu option for CI Type categories and subcategories is **Add New CI Type**.

Table 3: Right-click menu options

CI Types	Right-click menu options for these CI Types	Right-click menu options for most CIs belonging to these types
▪ Application Server ▪ Business Integration Software ▪ Database Server ▪ Directory Services ▪ Enterprise Applications ▪ Mail Services ▪ Other ▪ Portals ▪ Web Servers ▪ Generic Application ▪ ITAM - Asset Center ▪ Load Balancers	▪ Clone CI Type ▪ Add New Pattern ▪ Add New Monitor ▪ Add New Quick Monitor	▪ Delete Pattern ▪ Copy Pattern
▪ Web Server monitors	▪ Clone CI Type ▪ Add New Pattern ▪ Add New Monitor ▪ Add New Quick Monitor	▪ Delete Monitor ▪ Copy Monitor
▪	▪	▪
▪ NAT (Network Address Translation) ▪ Network Device ▪ Storage	▪ Add New Monitor ▪ Add New Quick Monitor	

CI Type Discovery Patterns

To enable discovery, the following information must be defined:

- Configuration Item (CI) types –Types of applications (for example, Apache Server, WebSphere) found in the business service.
- Discovery patterns that enable ServiceWatch to identify an application and its outgoing connections.

Defining discovery patterns for a CI type is a 2-part process:

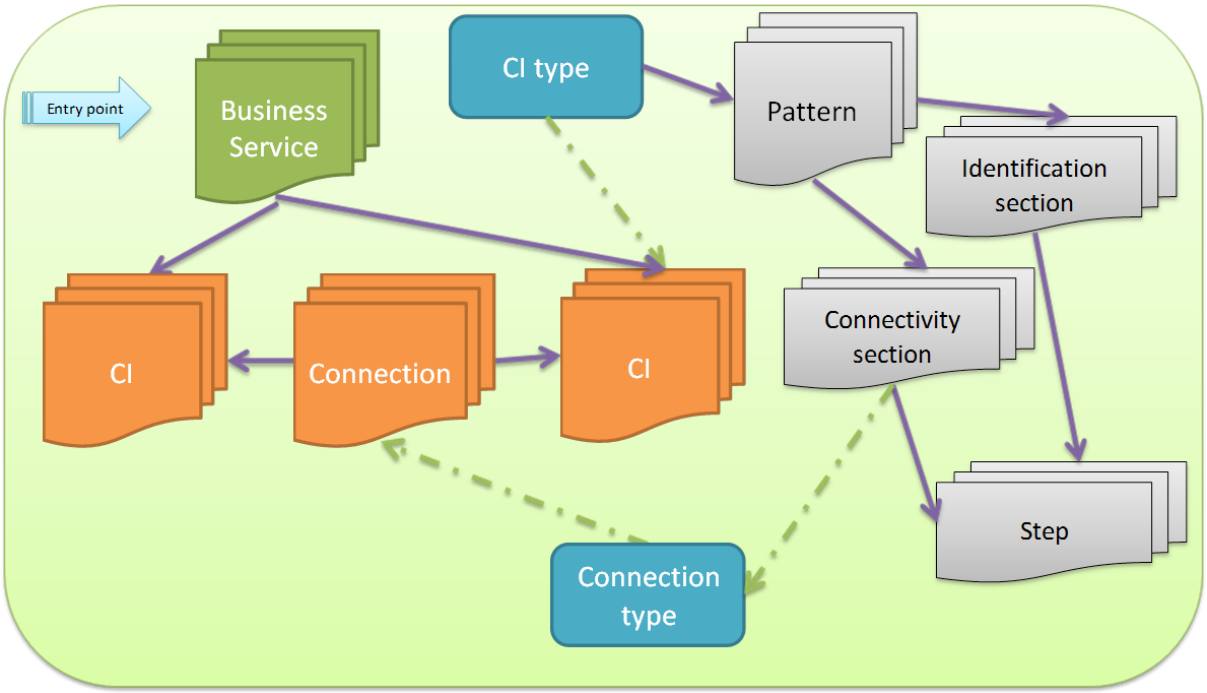
1. Defining descriptive information about the pattern and a list of its Identification sections and Connectivity sections.

- Identification sections identify entry point types that can point to the CI type.
- Connectivity sections identify types of outgoing connections to which that CI type can connect.

2. Defining the discovery Steps that must be performed for each identification section and connectivity section in that discovery pattern.

The workflow of this definition process is illustrated in Figure 66 and described in the *ServiceWatch Customization Guide*.

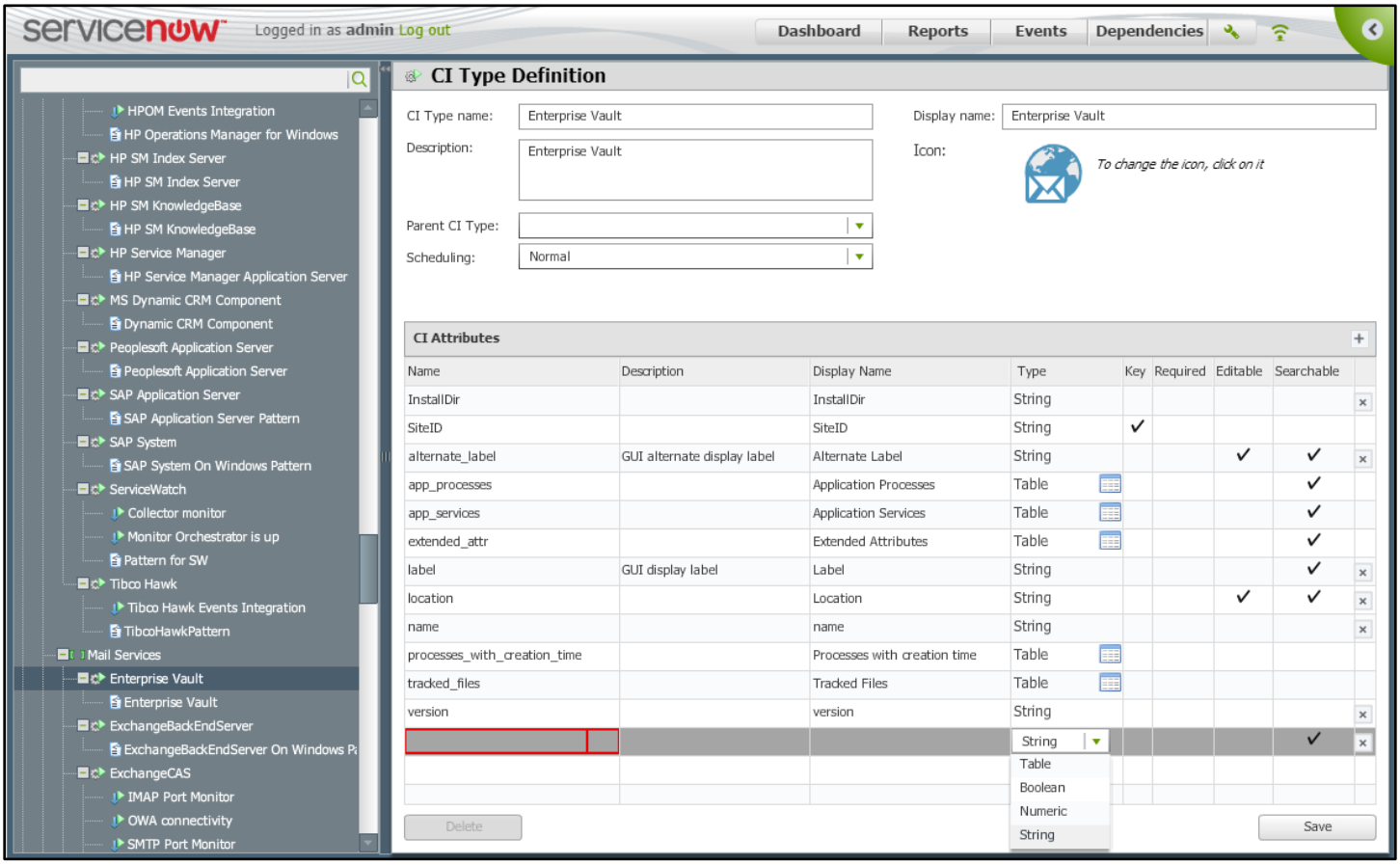
Figure 66: Workflow of the CI Type and Pattern definition process



The **CI Type Definition** window is shown in Figure 67.

CI Type Definition window

Figure 67: CI Type Definition window

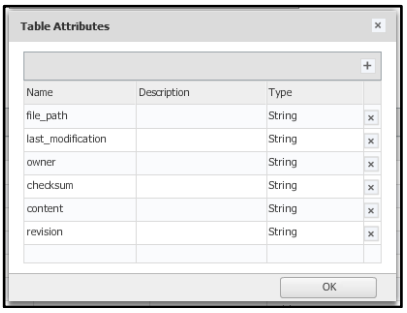


Note: When creating a *new* CI type, an identical but empty **CI Type Definition – New CI Type** window is displayed. After the CI type is saved, the **New CI Type** suffix is deleted from the window's name.

Click [+] in the **CI Attributes** header to add a row for defining an additional attribute. Click the **Type** column down-arrow to select **Table**, **Boolean**, **Numeric** or **String** from the drop-down list.

For a **Table** Type, click the Table icon to display the **Table Attributes** window with its own [+] button for adding table attributes.

Figure 68: CI Table Type – Table Attributes windows

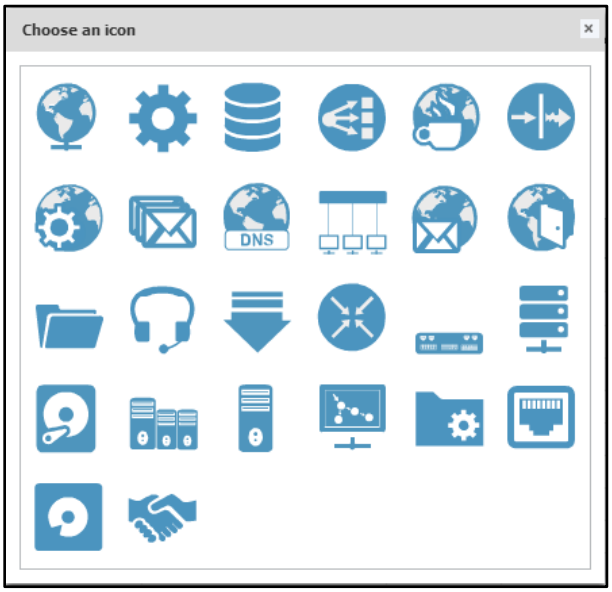


In the CI Type Definition window, click the **Key**, **Required**, **Editable** and/or **Searchable** columns to display a checkbox that can be selected.

Click [×] in the column on the right to remove its row from the table.

If you click the icon next to the text [To change the icon, click on it], the **Choose an Icon** window is displayed. Select the icon that best identifies the component.

Figure 69: Choose an icon window

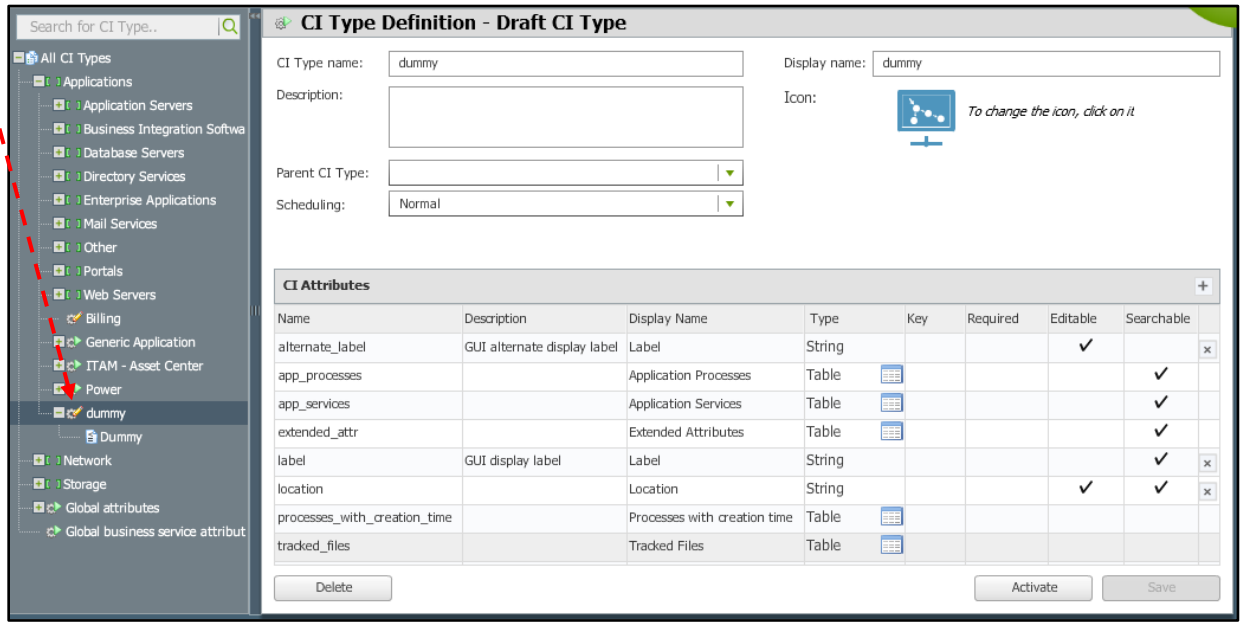


After creating or modifying the CI Type data, click [Save].

The suffix **- Draft CI Type** is added to the header of the **CI Type Definition** screen and a pencil icon [ ] is inserted next to the name of this CI Type in the **All CI Types** tree.

This CI Type remains inactive until you click [Activate] near the bottom right corner of the **CI Type Definition – Draft CI Type** screen.

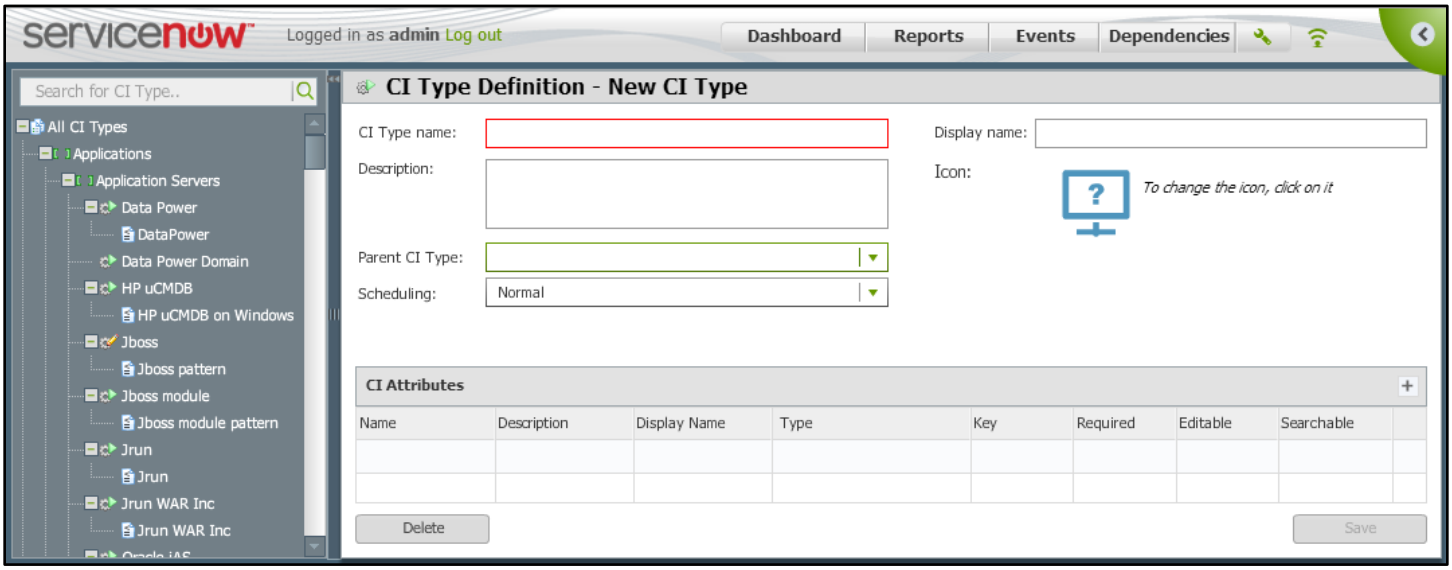
Figure 70: CI Type Definition – Draft CI Type screen



New CI Type Definition window

This window is displayed when the **Add New CI Type** option is selected in the **Knowledge Base > CI Types, Patterns & Monitors Definitions** right-click menu for an appropriate CI Type (see Table 2 on page 75).

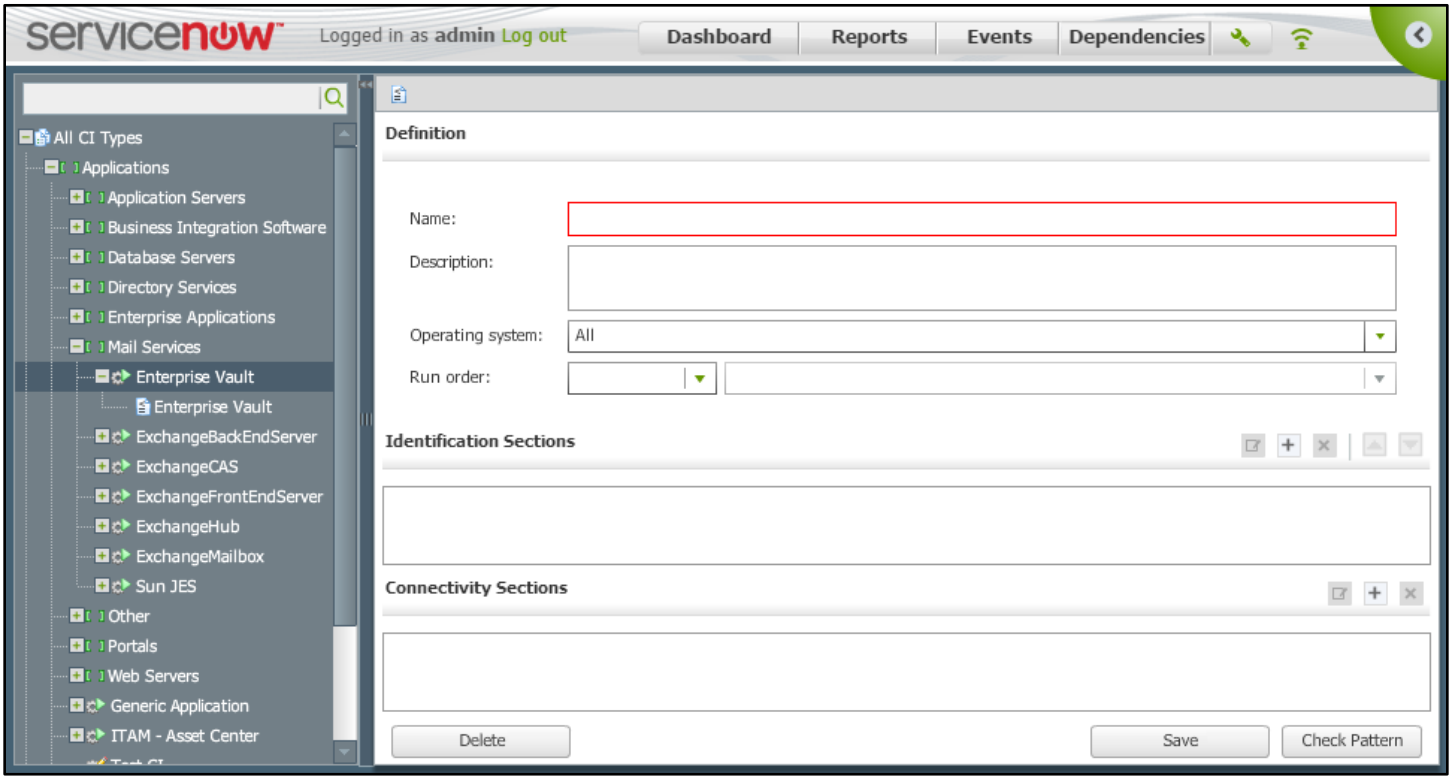
Figure 71: Add New CI Type window



New Pattern Window

This window is displayed when the **Add New Pattern** option is selected in the **Knowledge Base > CI Types, Patterns & Monitors Definitions** right click menu for an appropriate CI Type (see Table 3).

Figure 72: Add New Pattern window



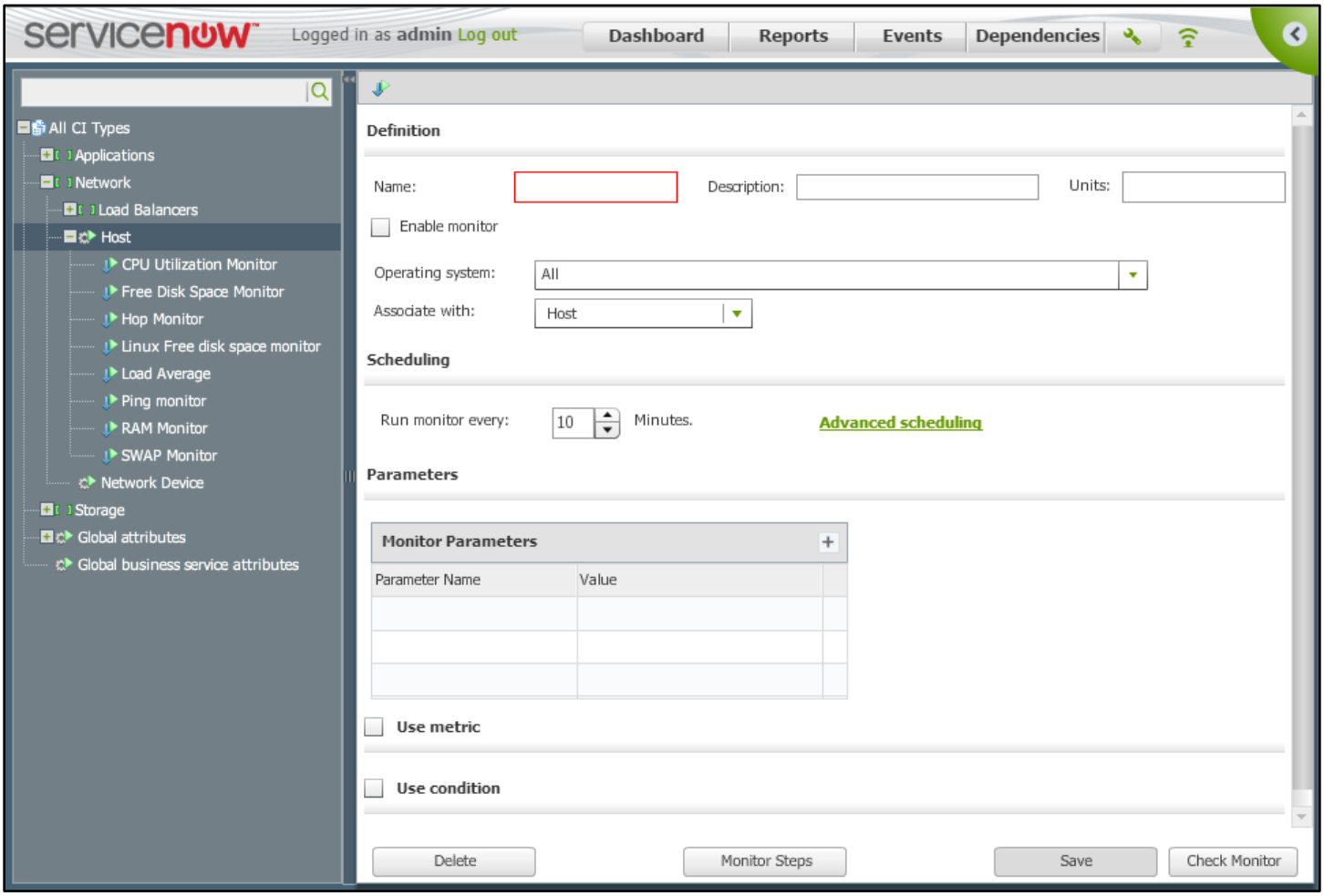
Restore Original option

The **Restore Original** option is an un-do mechanism that restores the factory default for CI Types that have a factory default.

Add New Monitor option

The **New Monitor** option manually defines a monitor that can perform the full range of monitoring tasks. For usage instructions, see the relevant text in Group & Business Service Monitors on page 86.

Figure 73: Add New Monitor window

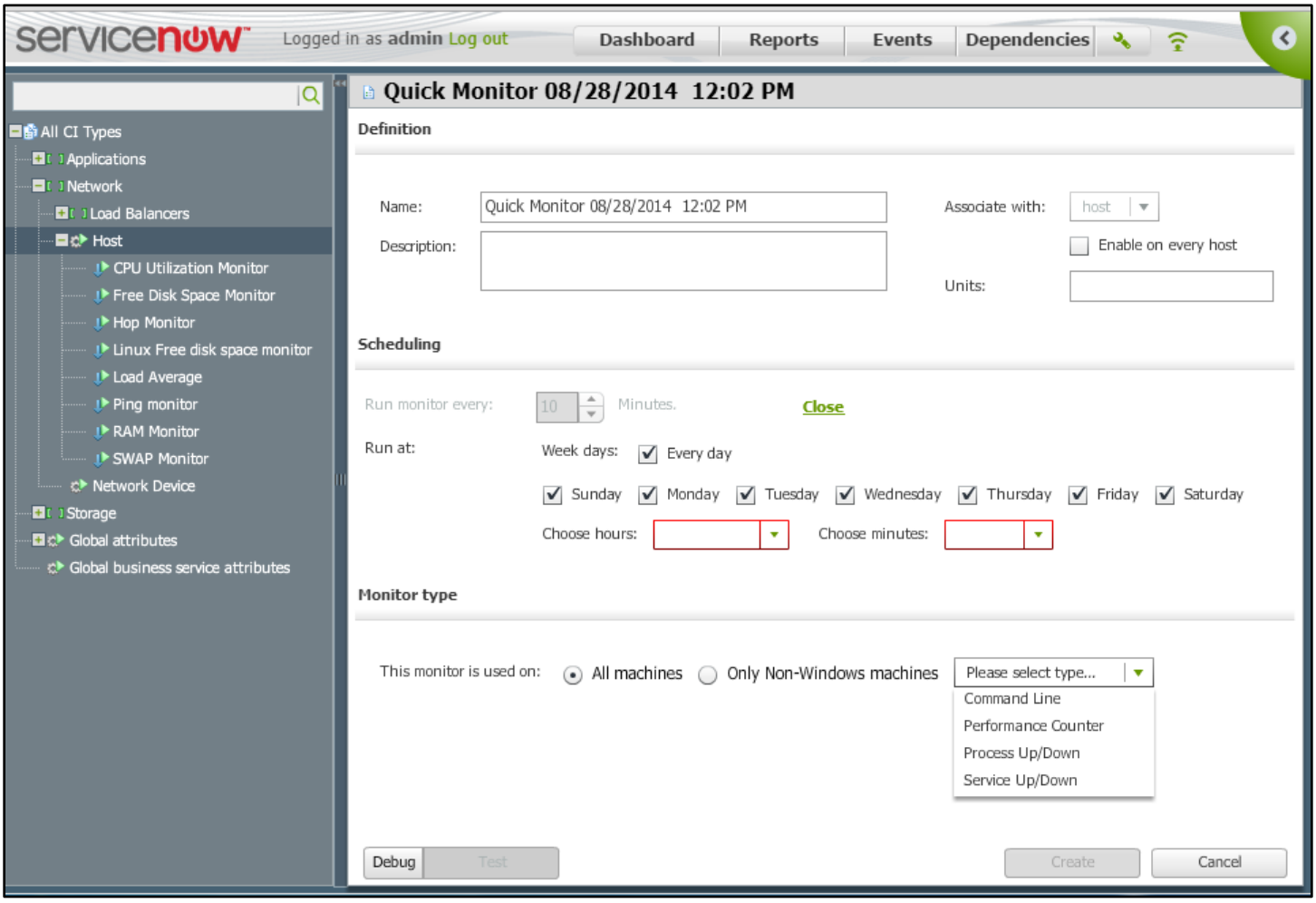


Add New Quick Monitor window

The **Quick Monitor** window manually defines a monitor that performs the most often required monitoring tasks. For instructions about using this window, see Group & Business Service Monitors on page 86.

The default name for each quick monitor is **Quick Monitor <dd/mm/yyyy hh:mm AM|PM>**. You can modify this name in the **Name** field.

Figure 74: Quick Monitor window

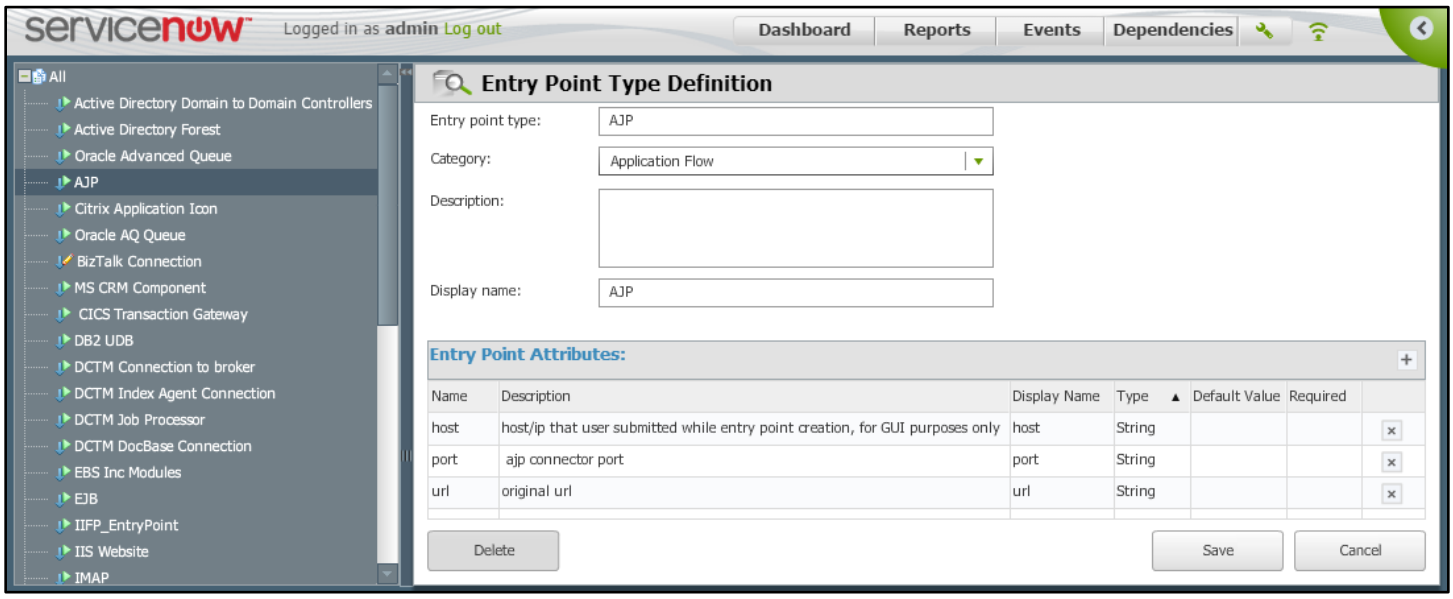


Entry Point Types

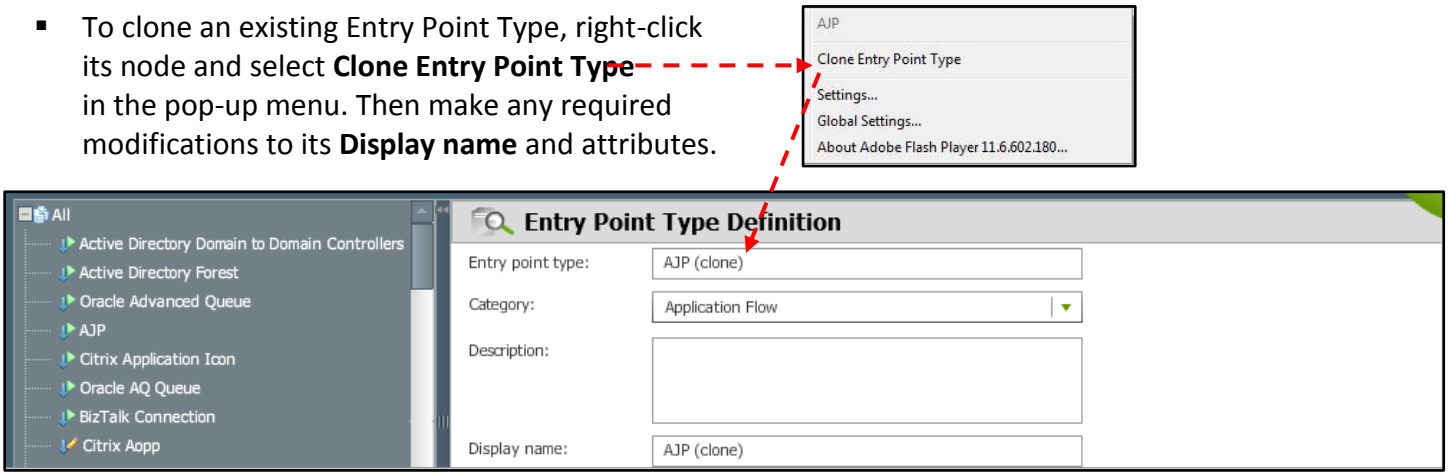
Click the **Entry Point Types** link in the **Settings** menu (Figure 64).

- To specify or modify the attributes of an existing Entry Point Type, click its node in the left panel of the displayed window.

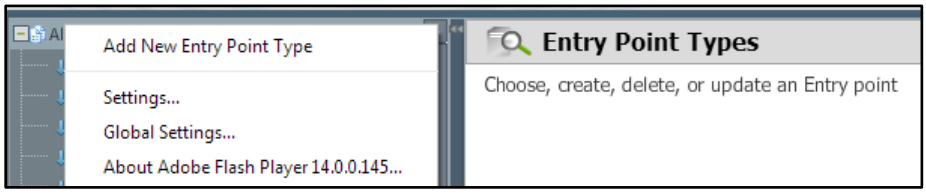
Figure 75: Displaying an Entry Point Type



- To clone an existing Entry Point Type, right-click its node and select **Clone Entry Point Type** in the pop-up menu. Then make any required modifications to its **Display name** and attributes.

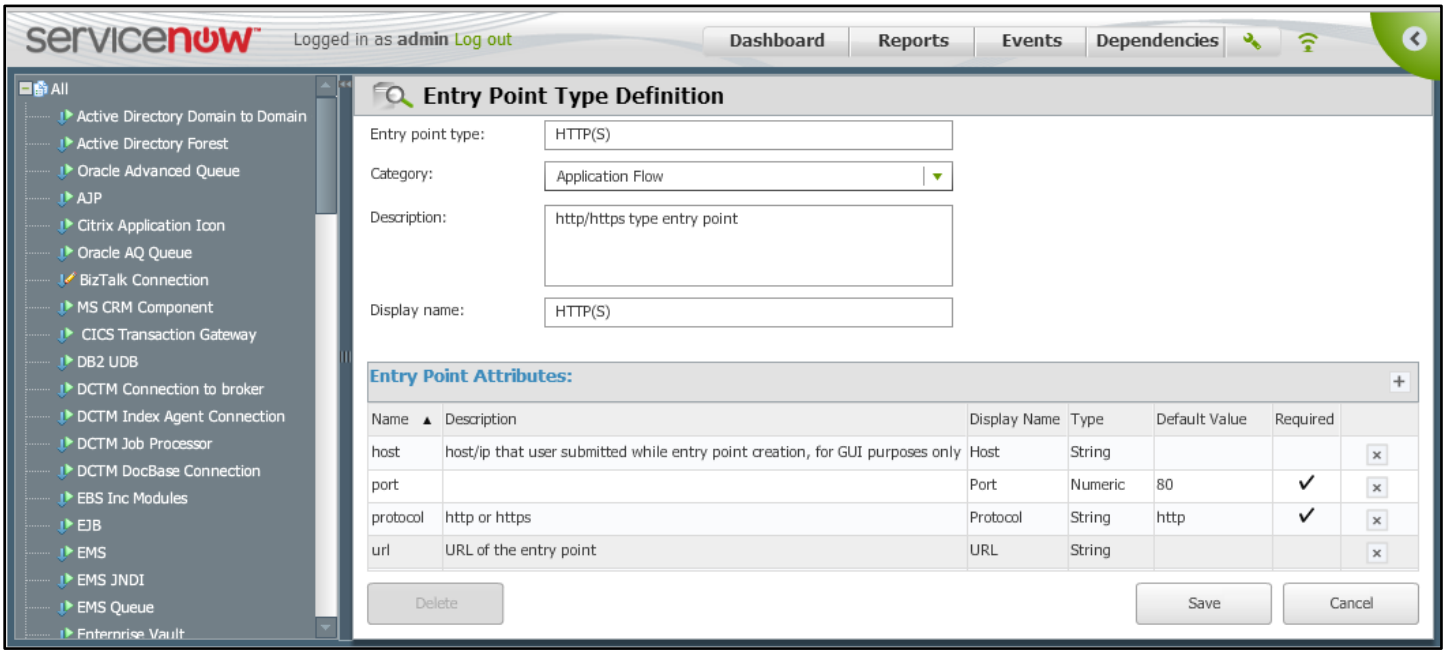


- To add a new Entry Point Type, right-click the **All** root of the Entry Point Type tree and select the **Add New Entry Point Type** option.



The Entry Point Type Definition screen is displayed.

Figure 76: Entry Point Type Definition screen



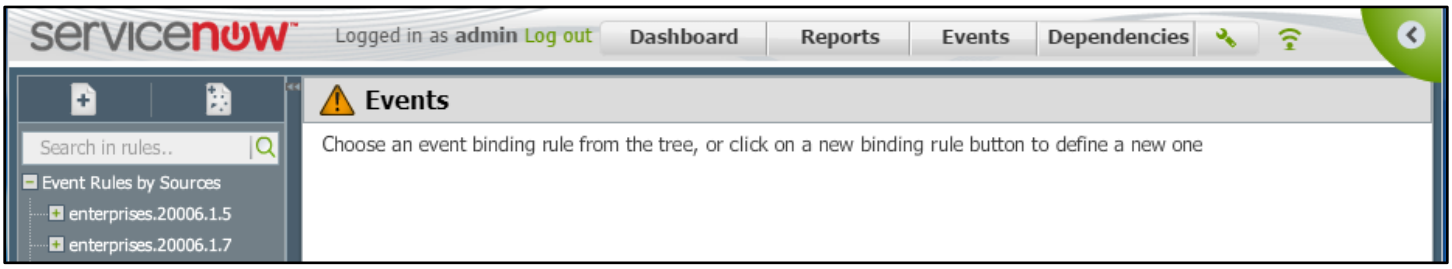
Click on the header of any column (except **Required**) in the **Entry Point Attributes** table to sort the table by that column. Click the same header again to reverse the sort order.

Modify the field values as required and click Save to produce a new entry point, or changes to an existing entry point, or an entry point similar to the one that was cloned.

Event Sources/Rules

Clicking the **Events Sources/Rules** link in the **Settings** menu (Figure 64) displays an empty **Events** window.

Figure 77: Events window with Event Rules by Sources tree

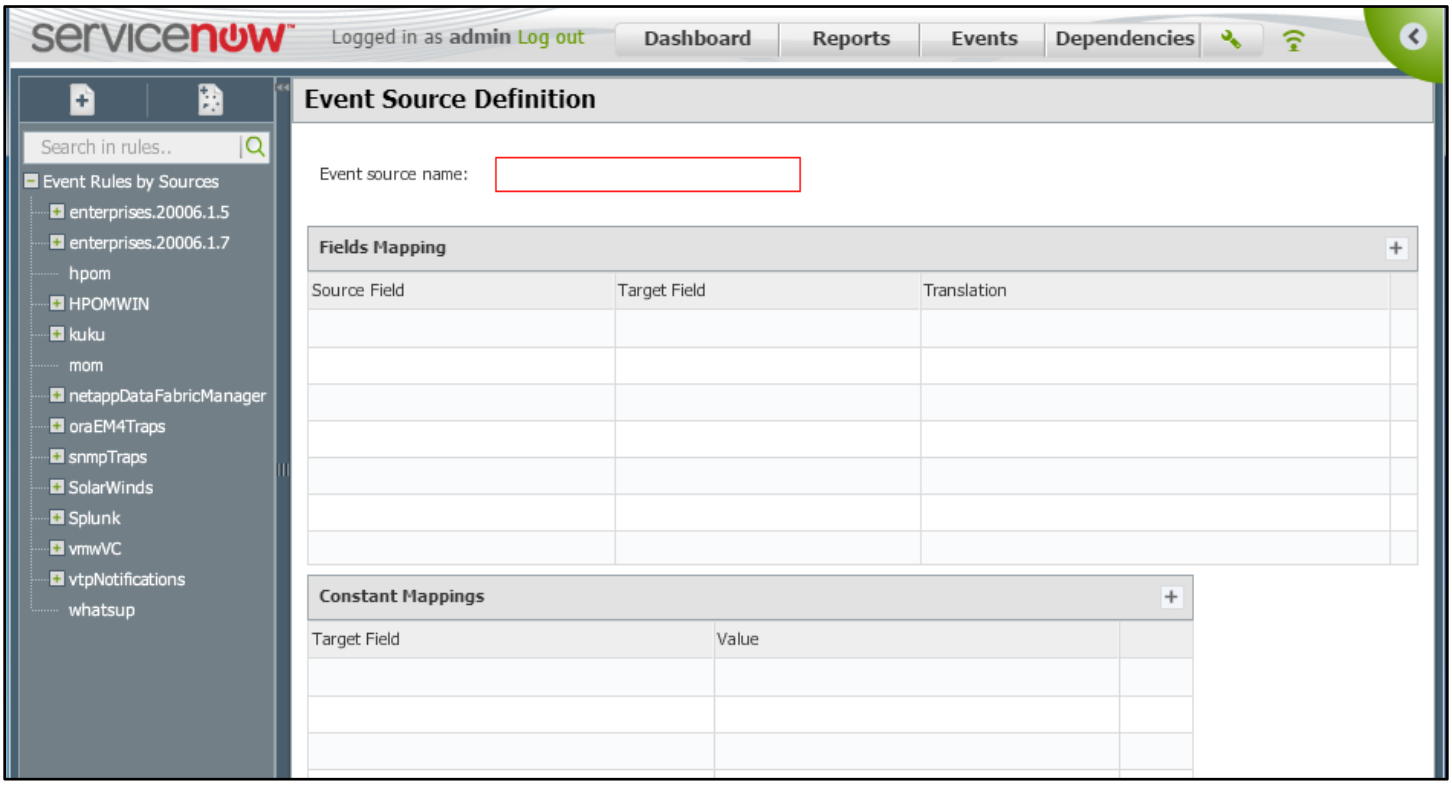


To edit the definition of an existing event source or binding rule, select it in the **Event Rules by Sources** tree. If you type a string in the Search box, only nodes with a rule that contains that string are displayed.

To delete an existing event source, right-click the source in the **Event Rules by Sources** tree and select the **Delete Event Source** option. To delete an existing event binding rule, right-click the rule in the **Event Rules by Sources** tree and select the **Delete Rule** option.

Click the icon to define a new event source. Click the icon to add a new binding rule to the set of translation and binding rules for unbound events from all event sources. If you click the icon, an empty **Event Source Definition** screen is displayed.

Figure 78: Event Source Definition screen

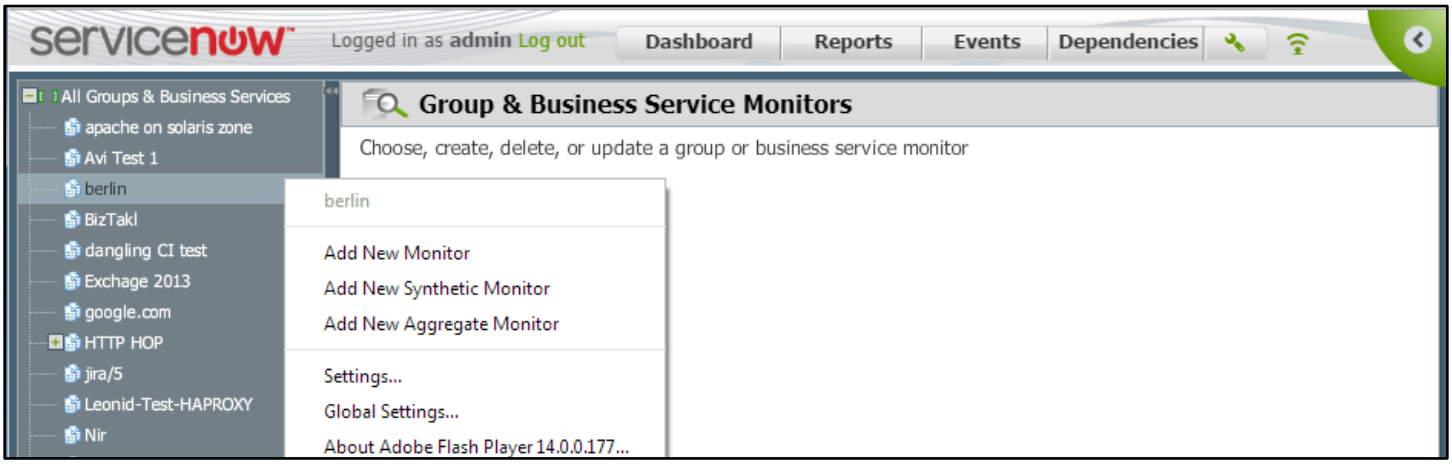


For information about defining event sources, defining event binding rules, configuring events, and integrating ServiceWatch with other event monitoring systems, see CHAPTER 7: CONFIGURING EVENTS.

Group & Business Service Monitors

Clicking the **Group & Business Service Monitors** link in the **Settings** menu (Figure 64) displays a window for creating, deleting and modifying aggregate, business service and Synthetic (user experience) monitors.

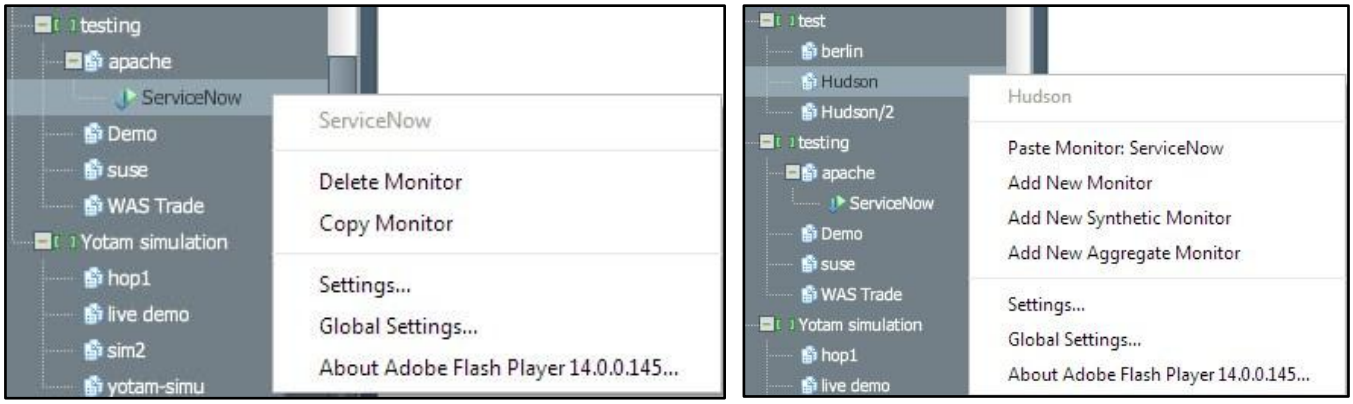
Figure 79: Group & Business Service Monitors window



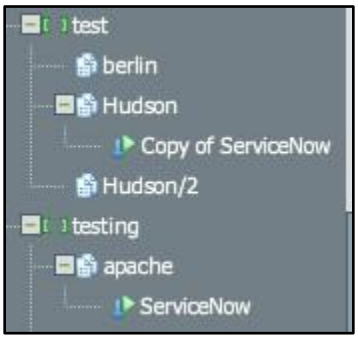
A business service monitor determines the health of a business service by examining the health status of each component of that service, evaluating the effect of that component's status on the status of the components 'above' it, and finally determining the cumulative effect on the health status of the business service as a whole.

By contrast, a Synthetic (user experience) monitor records the steps that are executed when performing the function to be monitored, then re-executes those steps periodically while recording the time required to perform each step and the response returned by that step.

To copy & paste an existing monitor, right-click the monitor and select the **Copy Monitor** option. Monitor data is copied to cache memory. Then right-click the recipient business service and select **the Paste Monitor <monitor name>** option.



A monitor with the name Copy of <monitor name> will be listed under the recipient business service's node.



To delete an existing monitor, right-click the monitor and select the **Delete Monitor** option.

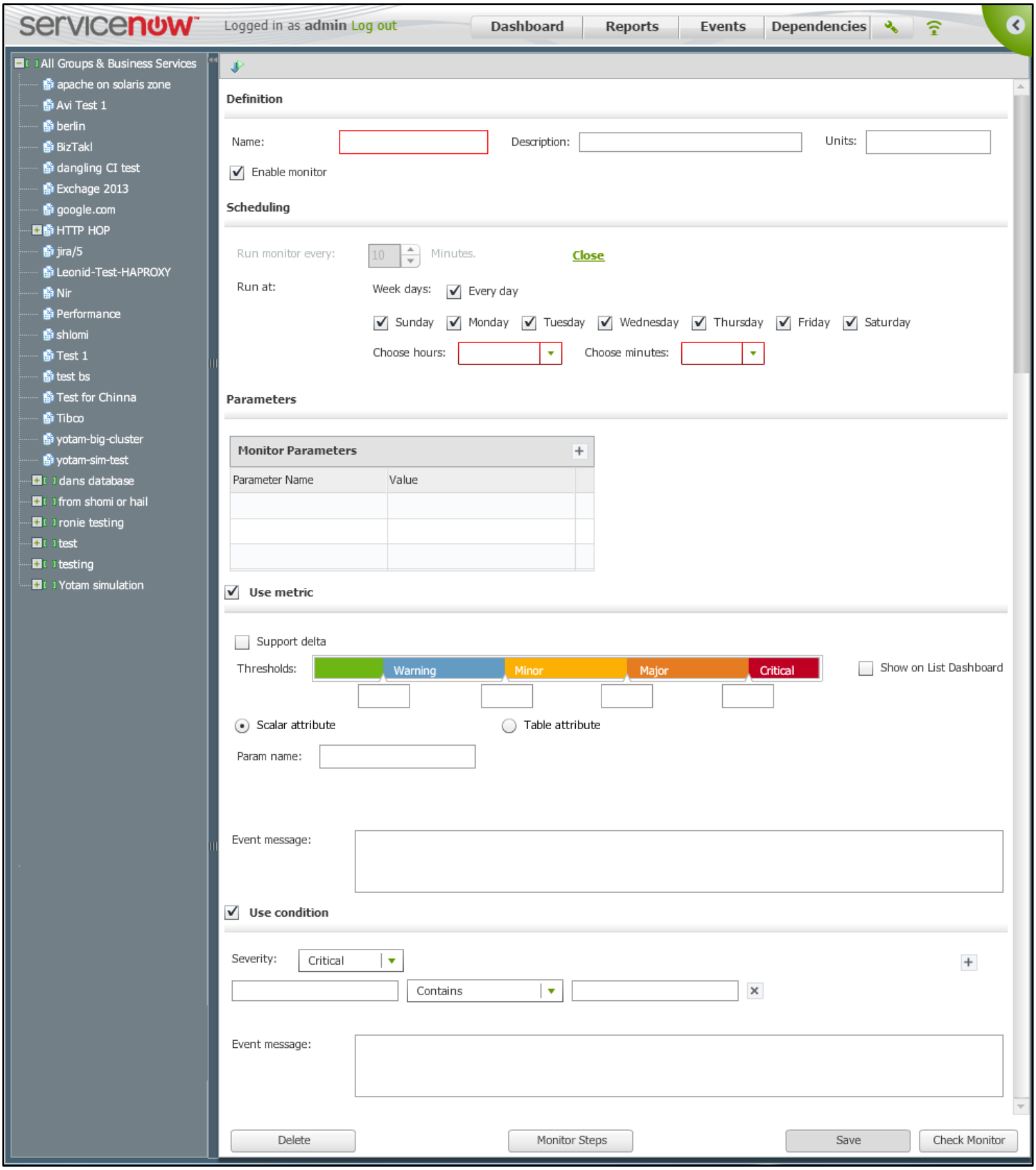
To add a group or business service monitor, right-click that group or business service and select the **Add New Monitor** option in the pop-up menu. The window shown in Figure 80 is displayed.

Appendix B of the *ServiceWatch Customization Guide* provides detailed information about how to define a monitor and the steps that are performed each time the monitor runs.

For information about using business service monitors, see CHAPTER 8: MONITORING BUSINESS SERVICES and the *ServiceWatch Customization Guide.*

For information about *aggregate* monitors, see Aggregate Monitors on page 187.
For information about Synthetic (user experience) monitors, see Synthetic Monitors on page 188.

Figure 80: Business Service Monitor Definition window



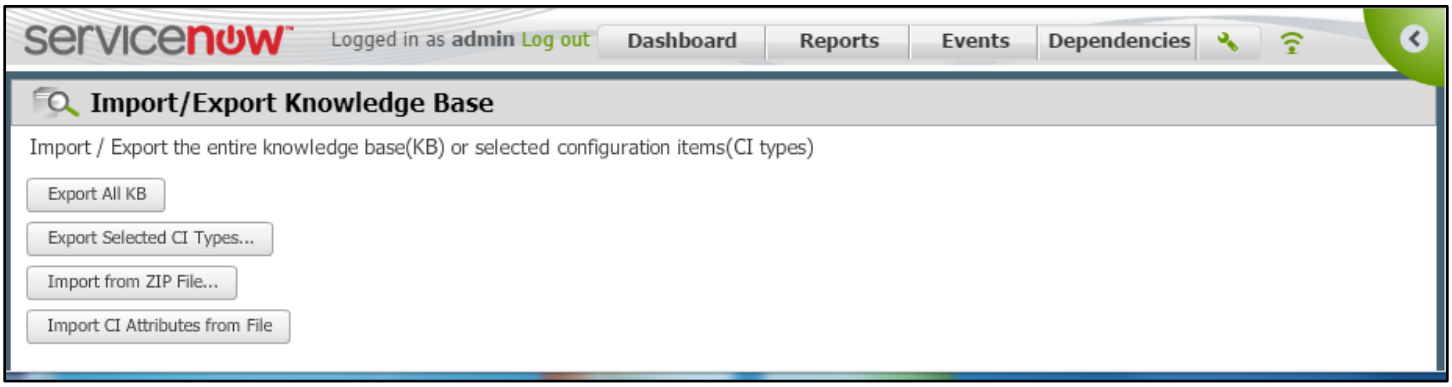
Import / Export

The import function enables you to receive new/updated ServiceWatch patterns. These patterns will override only unmodified patterns that were previously provided. If you have modified a pattern, it will not be replaced by an imported pattern.

The Export function enables you to export a pattern to other ServiceWatch environments and to send it to ServiceWatch Technical Support.

Clicking the **Import / Export** link in the **Settings** menu (Figure 64) displays the **Import / Export** window.

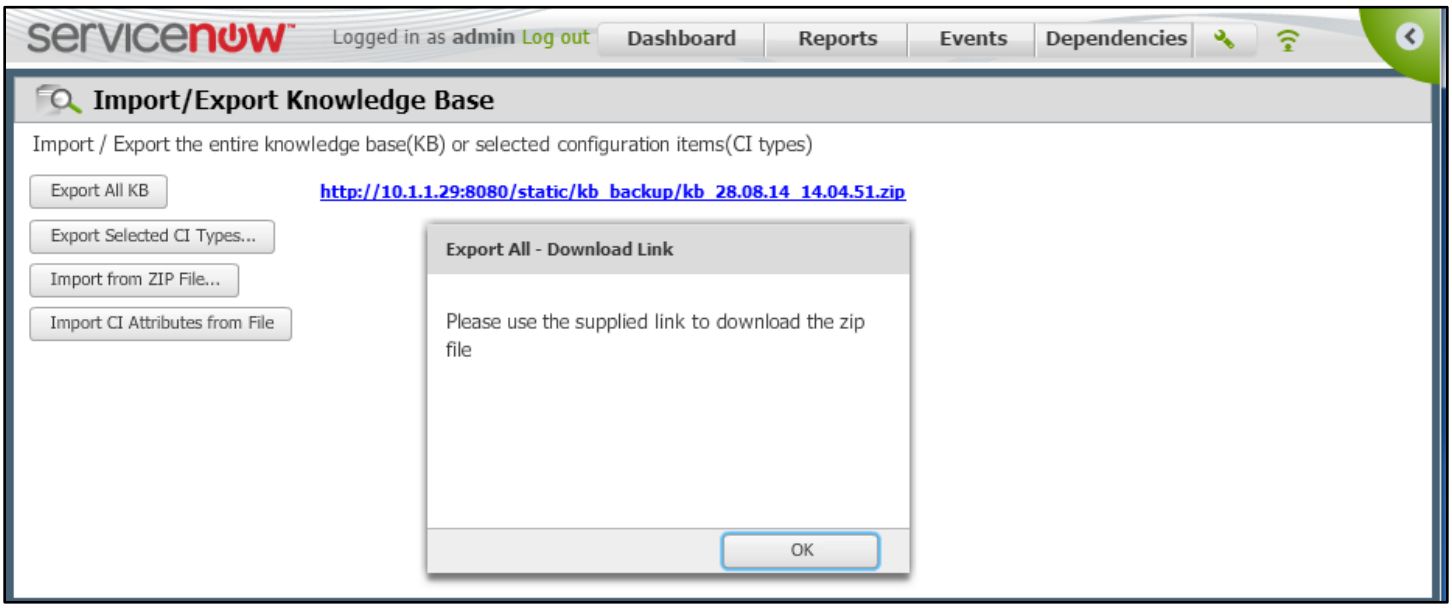
Figure 81: Import / Export Knowledge Base window



To export all of the CI Types in the Knowledge Base

Click Export All KB. A message box and a link to a zip file containing the parameters are displayed. If you click the link, you are given options to **Save**, **Save As**, or **Open** the file. Click **OK** to close the message box.

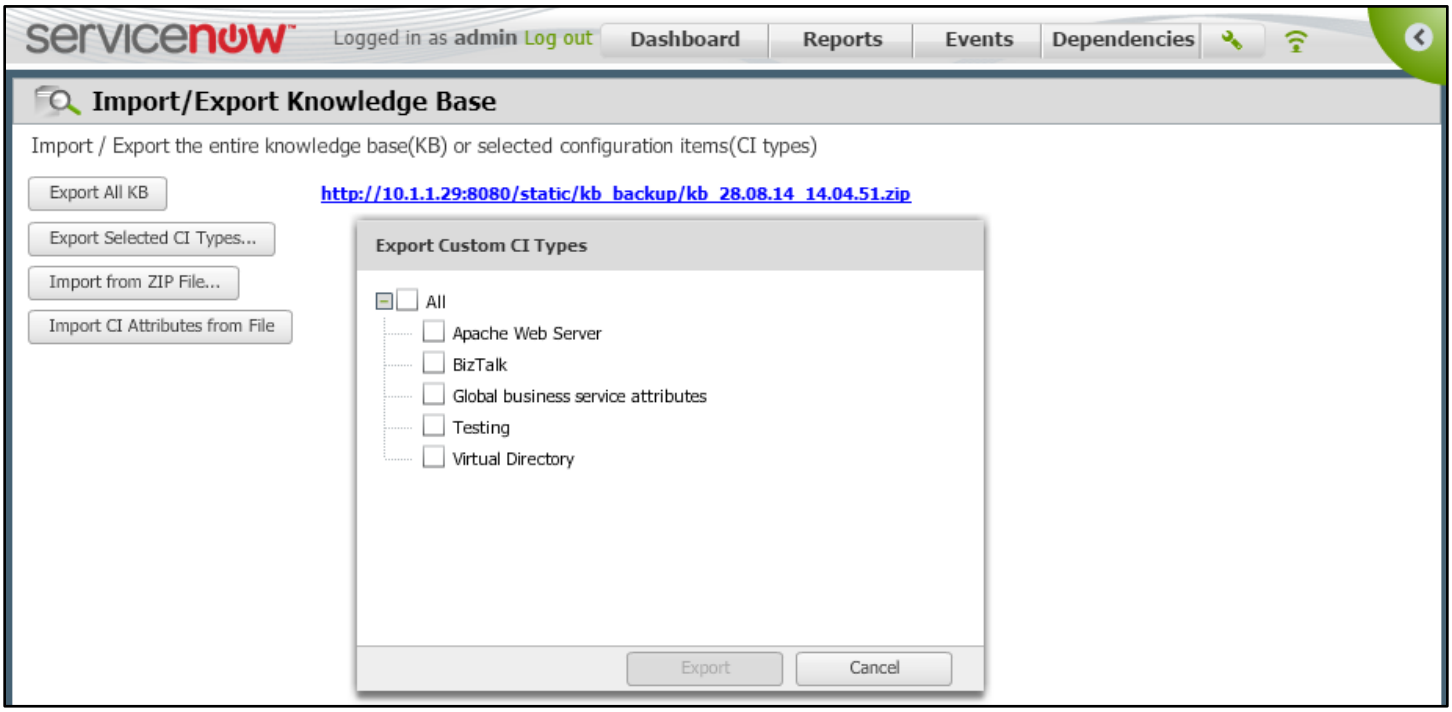
Figure 82: Export All Download Link message box



To export selected CI types

Click Export Selected CI Types... . An **Export Custom CI Types** message box is displayed.

Figure 83: CI Types Export Download Link message box

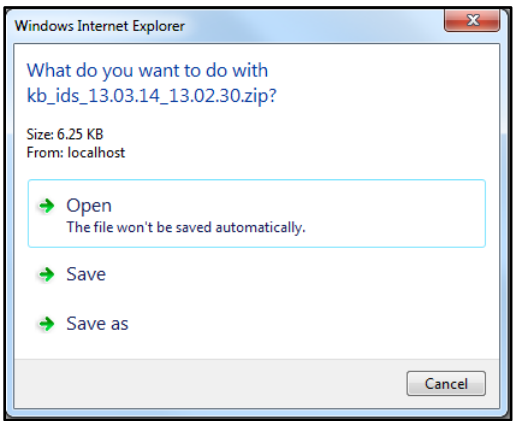


Select the checkboxes of the CI Types you want to export and click Export .

Download links are displayed. When you click the link to a file you want to download, a Windows dialog box gives you options to **Save**, **Save As** or **Open** the file.

Note: Only CI types with changed patterns are displayed in this file.

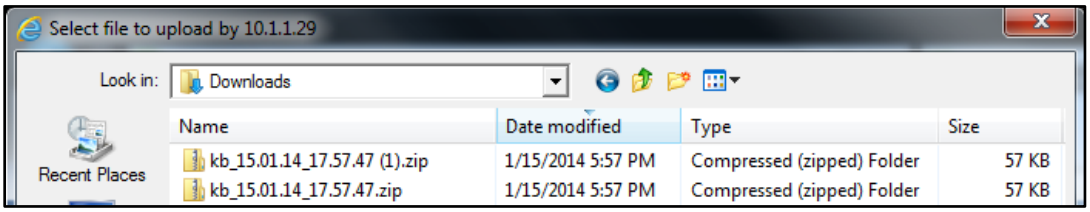
Figure 84: Open, Save, Save as dialog box



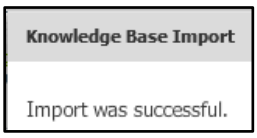
To import a previously exported file

Click Import from ZIP File... . An Explorer window lists the zip files available for import. You can double-click the file name to display its contents.

Figure 85: Zip files available for import



Select the file you want and click **Open**. You should receive an **Import was successful** message.



To import CI Attributes from a previously prepared CSV file

CSV File Format

The file must be in CSV format with fields and values in each line separated by a comma. If a value contains a comma, that value must be surrounded by quotes.

The first line of the CSV file must contain only the string **host** in the 1st field, the string **ci_type** in the 2nd field, and relevant existing global **key_attribute names** followed by updateable **attribute names** in the remaining fields.

In subsequent lines, the 1st field must contain a host name or IP address and the 2nd field must contain a CI type name (not a display name) unless a host is being updated. If the 2nd field is not populated, the system assumes the CI type is 'host'. The remaining fields contain key_attribute values (if any) followed by updatable attribute values. If an attribute is a key attribute for its CI type, its value is used to locate the relevant CI. Otherwise, its value is used to update the CI.

In theory, a file can contain as many subsequent lines as there are instances of that CI Type that can be identified by **host** and **key_attribute** values.

Attributes to be updated must be previously defined global attributes that can be edited. Attribute names can be taken from the specific CI type and from factory or user-defined global attributes.

Functionality

The system examines each line of the input file and locates CIs based on that line's key attributes. If any key attributes are missing, the system will update all of the CIs of the specified CI type on the specified host.

This feature's output includes error messages if the file contains an invalid format or if any line could not be processed for any reason. However, failure to process a line will not abort the update process. The output includes statistics on the number of CIs that were updated and the number of update attempts that failed.

Specified attributes that have a blank value are ignored. Therefore, a blank value cannot be used to remove an existing attribute value.

This feature cannot populate the attributes of an included CI based on the key attributes of its parent CI. For example, it is possible to populate the same attribute values on all WebSphere EARs that have the same name on the same host but not on an EAR of a specific WebSphere.

Operation

Click  **> Import / Export >** 

. A Browser window will open to enable you to select the CSV file to be imported. The import should run automatically when you select the input file. When the update process ends, you should receive the message: **Import finished. To view the import result, click** 

.

When you click the **Import Output** button, the run statistics are displayed. For example:

Import Log:

==========

Import Summary:

==========

Total data lines processed: *n*

CIs updated: *n*

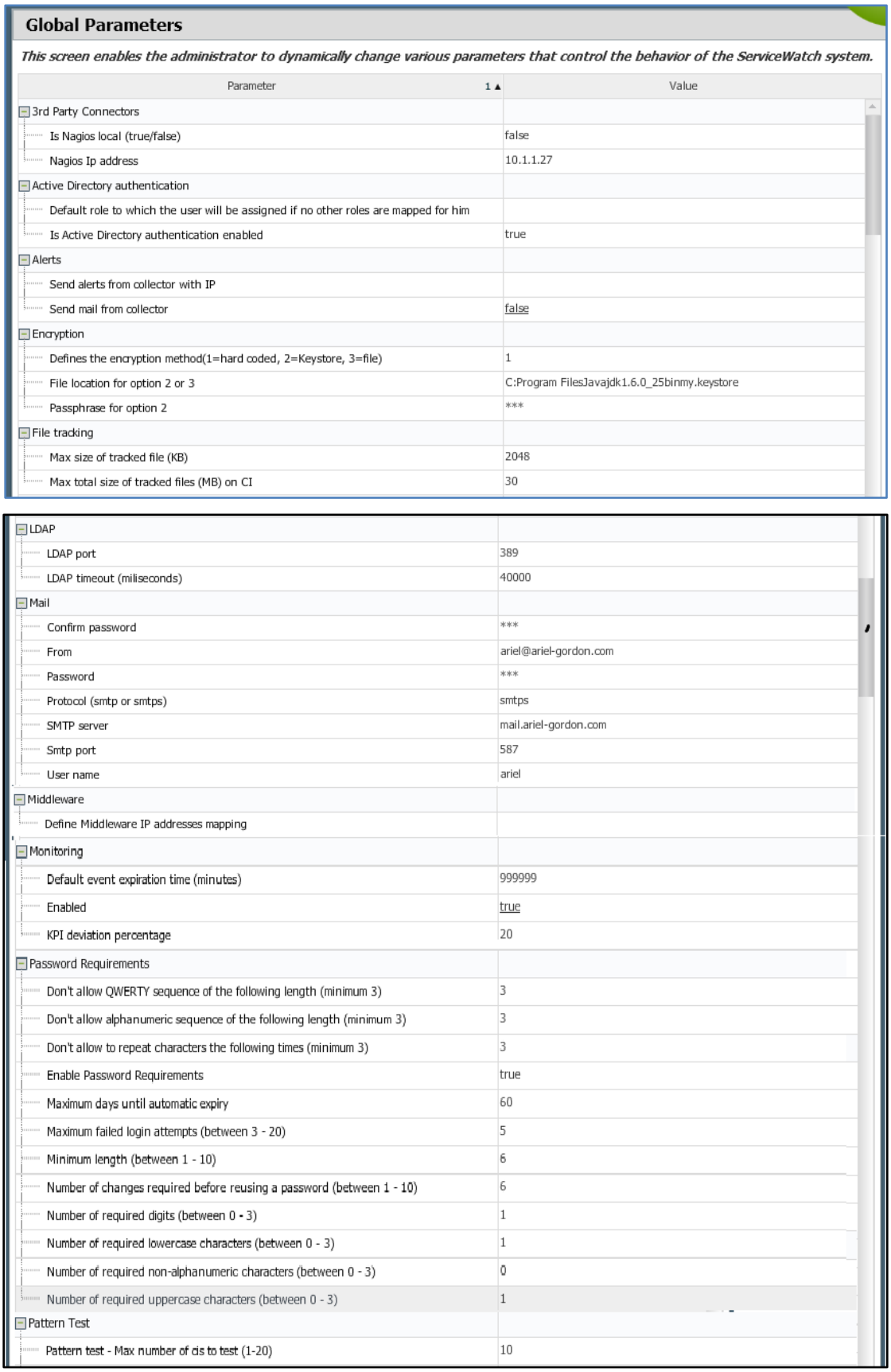
General settings

Global Parameters

This screen enables the administrator to dynamically change various parameters that control the behavior of the ServiceWatch system.

1. In the **General** area of the **Settings** menu (Figure 64), select the **Global Parameters** option. The screen for defining global system parameters is displayed (Figure 86). Included are parameters for defining:
   - ✓ 3rd Party Connectors
   - ✓ Active Directory authentication
   - ✓ Alerts
   - ✓ Encryption
   - ✓ File tracking
   - ✓ LDAP (Lightweight Directory Access Protocol)
   - ✓ Mail
   - ✓ Middleware
   - ✓ Monitoring
   - ✓ Password Requirements
   - ✓ Pattern Test
   - ✓ Rediscovery (incl. interval in minutes for Rare, Normal, and Frequent rediscovery)
   - ✓ Reports
   - ✓ SLA
   - ✓ SNMP (Simple Network Management Protocol) including the number of retries
   - ✓ SNMP Traps
   - ✓ SSH (Secure Shell)
   - ✓ System settings
   - ✓ Traffic based discovery
   - ✓ WMI (Windows Management Instrumentation)
2. To sort the Parameter types, click the **Parameter** heading. Click again to reverse the sort order.
3. Expand each Parameter type whose defaults you want to change. To alter a parameter's default, change its value to the desired default value.

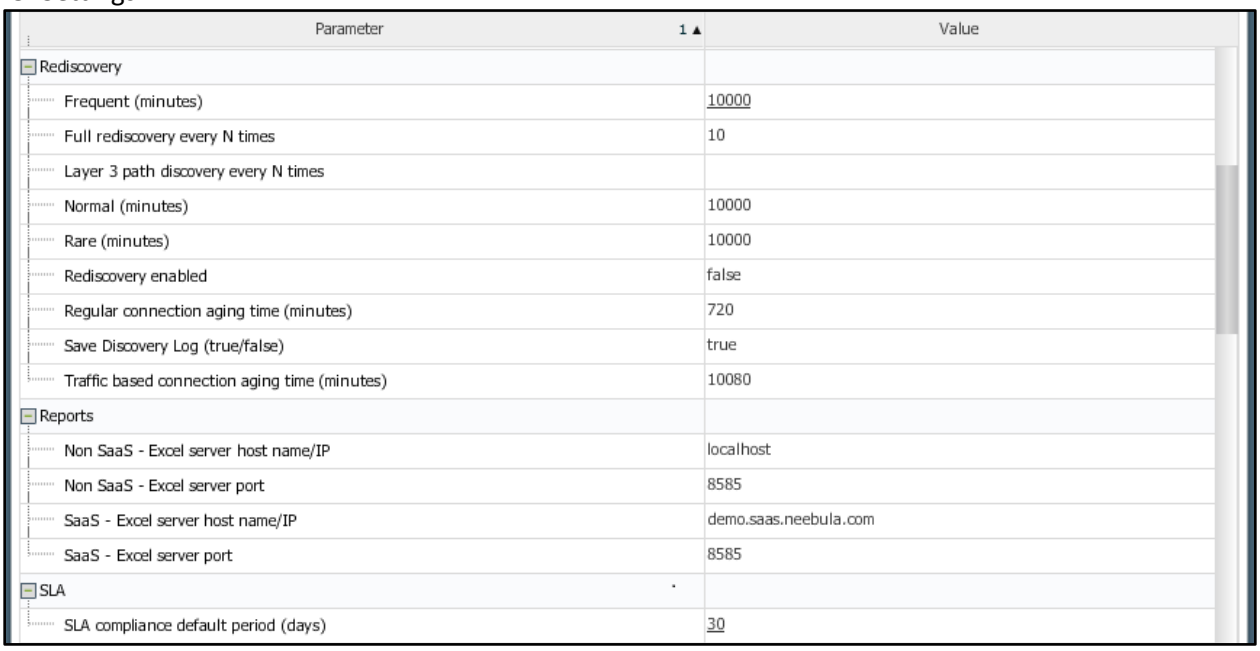
Figure 86: Global Parameters window (with all nodes expanded and sorted)



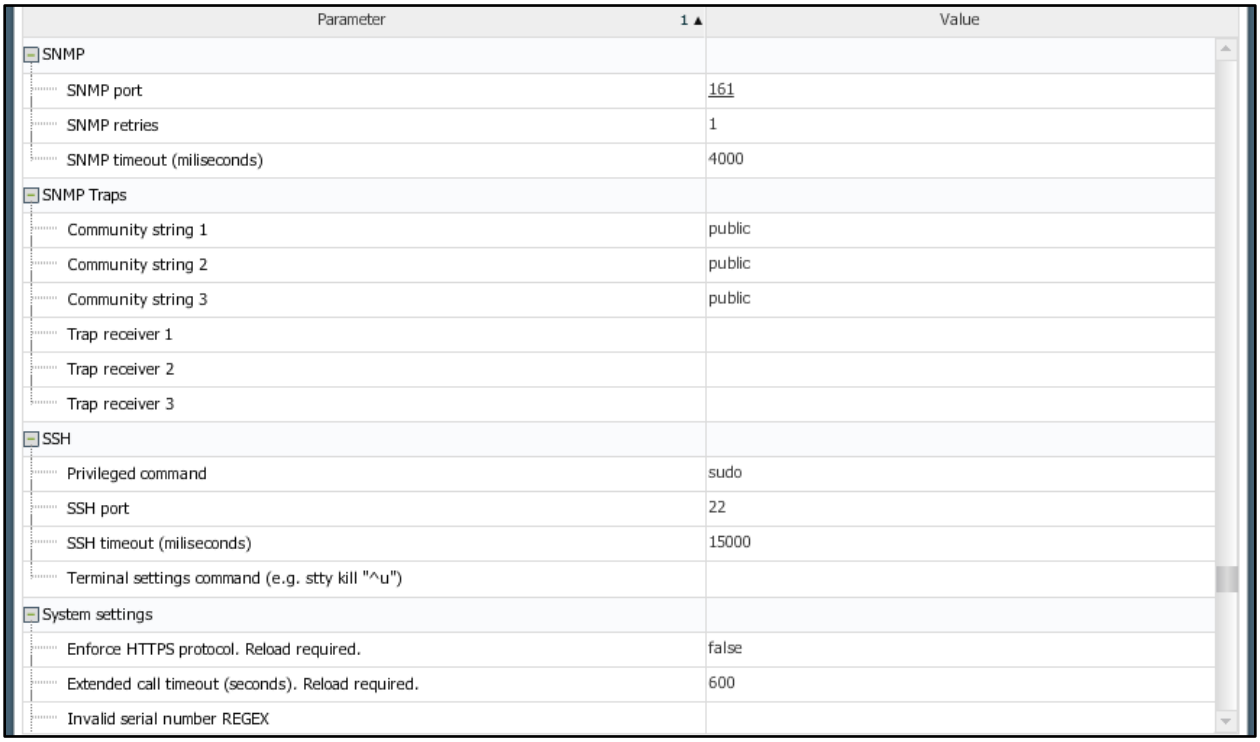
Global Parameters

This screen enables the administrator to dynamically change various parameters that control the behavior of the ServiceWatch system.

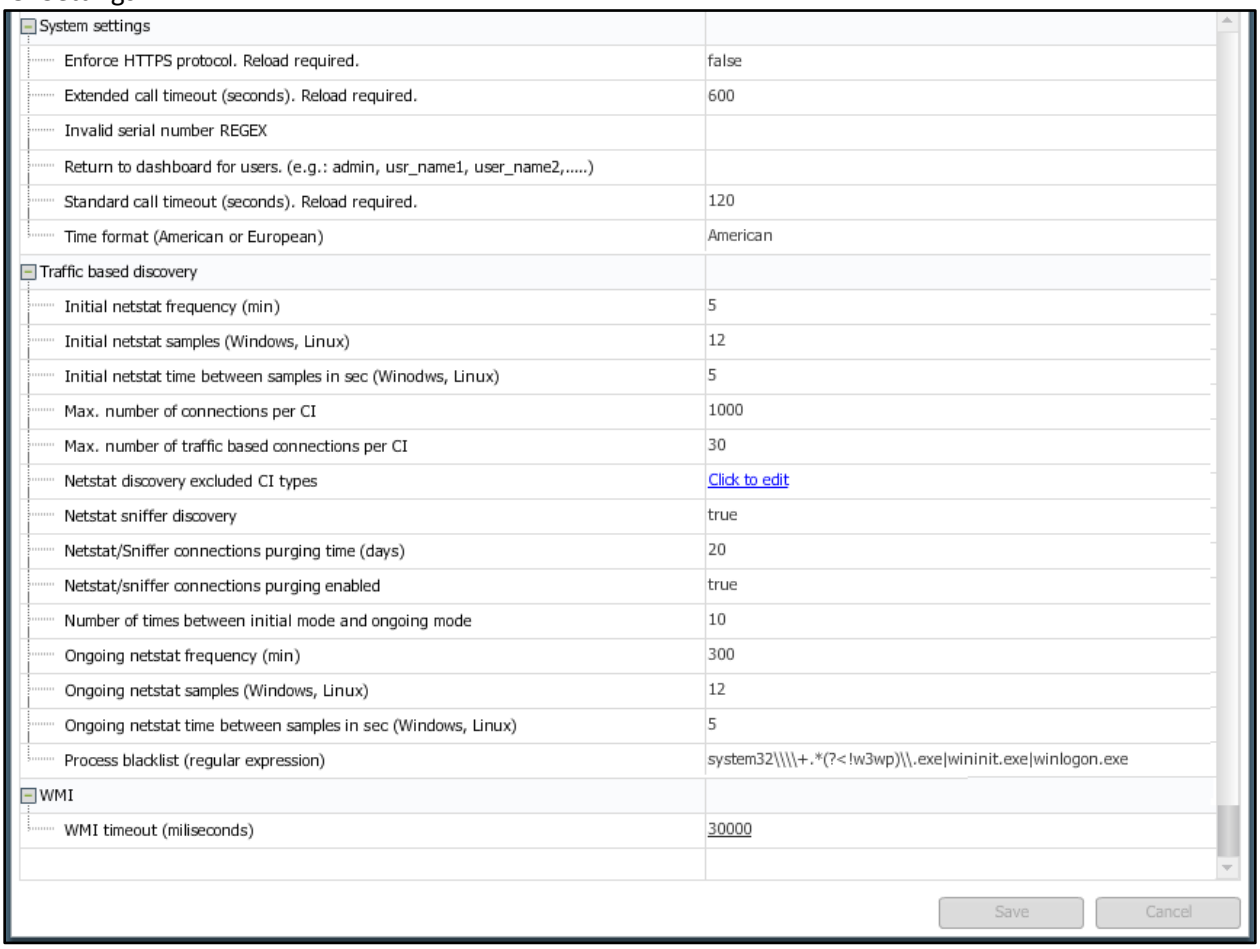
Parameter	Value
3rd Party Connectors	
Is Nagios local (true/false)	false
Nagios Ip address	10.1.1.27
Active Directory authentication	
Default role to which the user will be assigned if no other roles are mapped for him	
Is Active Directory authentication enabled	true
Alerts	
Send alerts from collector with IP	
Send mail from collector	false
Encryption	
Defines the encryption method(1=hard coded, 2=Keystore, 3=file)	1
File location for option 2 or 3	C:Program FilesJavajdk1.6.0_25binmy.keystore
Passphrase for option 2	***
File tracking	
Max size of tracked file (KB)	2048
Max total size of tracked files (MB) on CI	30
LDAP	
LDAP port	389
LDAP timeout (miliseconds)	40000
Mail	
Confirm password	***
From	ariel@ariel-gordon.com
Password	***
Protocol (smtp or smtps)	smtps
SMTP server	mail.ariel-gordon.com
Smtp port	587
User name	ariel
Middleware	
Define Middleware IP addresses mapping	
Monitoring	
Default event expiration time (minutes)	999999
Enabled	true
KPI deviation percentage	20
Password Requirements	
Don't allow QWERTY sequence of the following length (minimum 3)	3
Don't allow alphanumeric sequence of the following length (minimum 3)	3
Don't allow to repeat characters the following times (minimum 3)	3
Enable Password Requirements	true
Maximum days until automatic expiry	60
Maximum failed login attempts (between 3 - 20)	5
Minimum length (between 1 - 10)	6
Number of changes required before reusing a password (between 1 - 10)	6
Number of required digits (between 0 - 3)	1
Number of required lowercase characters (between 0 - 3)	1
Number of required non-alphanumeric characters (between 0 - 3)	0
Number of required uppercase characters (between 0 - 3)	1
Pattern Test	
Pattern test - Max number of cis to test (1-20)	10



Parameter	Value
Rediscovery	
Frequent (minutes)	10000
Full rediscovery every N times	10
Layer 3 path discovery every N times	
Normal (minutes)	10000
Rare (minutes)	10000
Rediscovery enabled	false
Regular connection aging time (minutes)	720
Save Discovery Log (true/false)	true
Traffic based connection aging time (minutes)	10080
Reports	
Non SaaS - Excel server host name/IP	localhost
Non SaaS - Excel server port	8585
SaaS - Excel server host name/IP	demo.saas.neebula.com
SaaS - Excel server port	8585
SLA	
SLA compliance default period (days)	30



Parameter	Value
SNMP	
SNMP port	161
SNMP retries	1
SNMP timeout (miliseconds)	4000
SNMP Traps	
Community string 1	public
Community string 2	public
Community string 3	public
Trap receiver 1	
Trap receiver 2	
Trap receiver 3	
SSH	
Privileged command	sudo
SSH port	22
SSH timeout (miliseconds)	15000
Terminal settings command (e.g. stty kill "^u")	
System settings	
Enforce HTTPS protocol. Reload required.	false
Extended call timeout (seconds). Reload required.	600
Invalid serial number REGEX	



4. When done, click Save, or click Cancel.to exit without saving any changes.

Table 4: Global Parameters

Parameter Type	Parameter	Description, Comment or Typical Value
3rd Party Connectors		
Is Nagios local (true/false)		NetSaint **>** **N**agios **A**in't **G**onna **I**nsist **O**n **S**ainthood acronym
Nagios IP address		
Active Directory authentication		
Default role for every user who does not have any assigned role		Click > **Roles** to view a table of currently defined roles. Click **+** in the table's top right corner to define a new Role.
Is Active Directory authentication enabled		Valid values: true *or* false
Alerts		
Send alerts from collector with IP		Valid values: true *or* false
Send mail from collector		Valid values: true *or* false

Parameter Type	Parameter	Description, Comment or Typical Value
Encryption		
Defines the encryption method: 1 = hard coded, 2 = KeyStore, 3 = file		1
File location for option 2 or 3		C:Program FilesJavajdk1.6.0_25binmy.keystore
Passphrase for option 2		
File tracking		
Max size for each tracked file (KB)		2048
Max total size of tracked files (MB) on CI.		30
LDAP		
LDAP port		389
LDAP timeout (milliseconds)		If the LDAP timeout interval is exceeded, ServiceWatch cannot connect to the LDAP server. This may adversely affect authentication using LDAP. Typical value: 40000
Mail		
Confirm password		
From		
Password		
Protocol (SMTP *or* SMTPS)		
SMTP server		Name or IP address of the SMTP server
SMTP port		
User name		Name of the user who should receive the email
Middleware		
Define Middleware IP addresses mapping		
Monitoring		
Default event expiration time (minutes)		If not set, the default is 999,999 minutes. Typical: 10079
Enabled		true
KPI deviation percentage		20

Parameter Type	Parameter	Description, Comment or Typical Value
Password Requirements		
Don’t allow QWERTY sequence of the following length (minimum 3)		3
Don’t allow alphanumeric sequence of the following length (minimum 3)		3
Don’t allow to repeat characters the following times (minimum 3)		3
Enforce security restrictions		true
Maximum days until automatic expiry		Default: 60
Maximum failed login attempts (between 3 - 20)		5
Minimum length (between 1 – 10)		6
Number of changes required before reusing a password (between 1 – 10)		6. If not set, passwords can be reused immediately.
Number of required digits (between 0 - 3)		If set to zero, these digits and characters are not required in new passwords.
Number of required lowercase characters (between 0 – 3)		
Number of required non-alphanumeric characters (between 0 – 3)		
Number of required uppercase characters (between 0 – 3)		
Rediscovery		
Frequency (minutes)		Value must be set and must be 5 or more. Typical: 60
Full rediscovery every N times		Rediscovery involves specific business elements. Full rediscovery involves the entire business service. 10
Layer 3 path discovery every N times		Network elements discovery
Normal (minutes)		360
Rare (minutes)		Suitable for CIs that rarely change. 2400
Rediscovery enabled		Valid values: true, false
Regular connection aging time in minutes (0 means no aging)		Time after which non-used netstat connections are removed.
Save Discovery Log (true/false)		
Traffic based connection aging time in minutes (0 means no aging)		Time after which non-used traffic connections are removed.

Parameter Type	Parameter	Description, Comment or Typical Value
Reports		
Non SaaS - Excel server host name/IP		local host. Provide values for either the pair of SaaS or Non-SaaS parameters but not for both pairs.
Non SaaS - Excel server port		8585
SaaS - Excel server host name/IP		Provide values for either the pair of SaaS or Non-SaaS parameters but not for both pairs.
SaaS - Excel server port		
SLA		
SLA compliance default period (days)		Default interval for determining SLA compliance. Value must be more than zero. Typical: 30
SNMP		
SNMP port		
SNMP retries		1
SNMP timeout (milliseconds)		4000
SNMP Traps		
Community string 1		Example: When an SNMP trap is set to receiver 1, community string 1 is put in that trap.
Community string 2		
Community string 3		
Trap receiver 1		Alerts can be sent as SNMP traps. Up to 3 receivers are supported. When a receiver is set, the SNMP trap is sent to that receiver using the corresponding community string.
Trap receiver 2		
Trap receiver 3		
SSH		
Privileged command		For example, **sudo** (**s**uper-**u**ser **do** command).
SSH port		20
SSH timeout (milliseconds)		If value is exceeded, SSH connections will not be opened and discovery of Linux/Unix devices will not occur. Value must be 500 or more. Typical: 60000
Terminal settings command (e.g., stty kill ^u)		Systems with non-standard terminal settings can cause problems when using SSH. This parameter enables terminal setting commands to be executed during SSH session initialization. For Windows, see https://www.mkssoftware.com/docs/man1/stty.1.asp For UNIX , see http://unixhelp.ed.ac.uk/CGI/man-cgi?stty

Parameter Type	Parameter	Description, Comment or Typical Value
System settings		
Enforce HTTPS protocol. Reload required.		false. If this parameter is changed, restart the server.
Extended call timeout (seconds). Reload required.		Default value: 180. Change takes effect after application is restarted.
Invalid serial number REGEX		Error message format of the serial number command. Its value consists of strings using | as the delimiter.
Return to dashboard for users. (e.g., admin, user_name1, user_name2,...)		After a time interval, the Dashboard is automatically displayed for the specified users (comma separated).
Standard call timeout (seconds). Reload required.		Default value: 30. Change takes effect when application is restarted.
Time format (American *or* European)		Date & time format. American = mm/dd/yyyy hh:mm:ss European = dd/mm/yyyy hh:mm:ss
Traffic based discovery		
Initial netstat frequency (min)		5. Time interval after which Netstat discovery is performed.
Initial netstat samples (Windows, Linux)		12
Initial netstat time between samples in sec (Windows, Linux)		5
Max. number of connections per CI		1000
Max. number of traffic based connections per CI		30
Netstat discovery excluded CI types		Multiple CI types are comma separated.
Netstat sniffer discovery		Default: true; if false, all generic patterns are disabled.
Netstat/Sniffer connections purging time (days)		20. Number of days after which connection stats are deleted
Netstat/sniffer connections purging enabled		true
Number of times between initial mode and ongoing mode		10. The first time a host is discovered, netstat discovery is based on **Initial netstat frequency & samples.** Afterwards, the mode is set to **ongoing** and discovery is based on **Ongoing netstat frequency** & **samples**.
Ongoing netstat frequency (min)		300

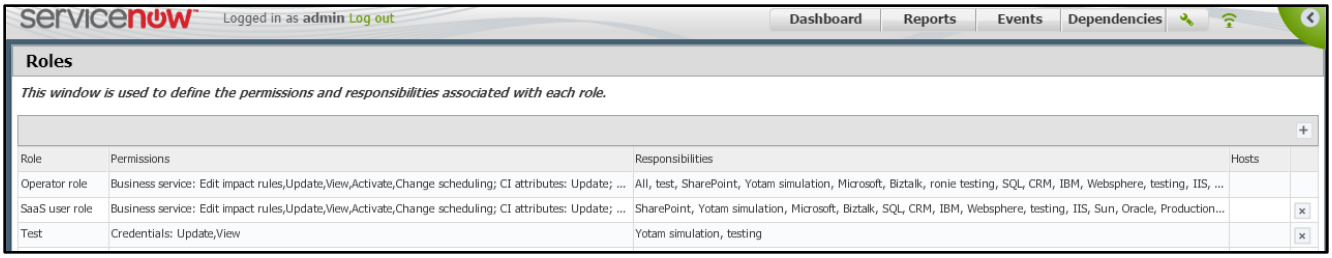
Parameter Type	Parameter	Description, Comment or Typical Value
Ongoing netstat samples (Windows, Linux)		12
Ongoing netstat time between samples in sec (Windows, Linux)		5
Process blacklist (regular expression)		system32\\\\+.*(?<!w3wp)\\.exe|wininit.exe|winlogon.exe indicates outgoing connections from processes are not created.
WMI		
WMI timeout (milliseconds)		180000

Active Directory feature (LDAP)

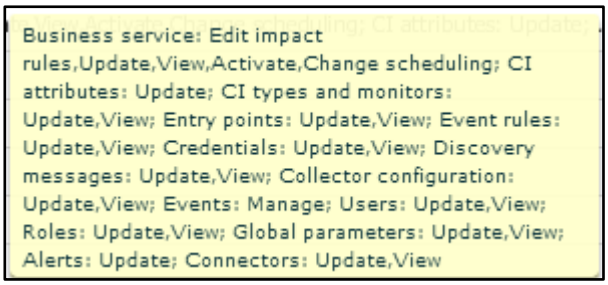
To use the LDAP Active Directory feature:

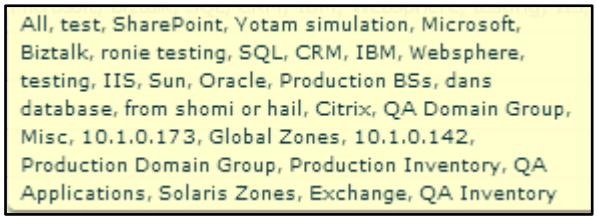
1. Expand the Active directory authentication node in the Global Parameters window and set **Is Active Directory authentication enabled** to true.
2. Click Save.
3. Select **Settings → Roles** to display the **Roles** window.

Figure 87: Roles window



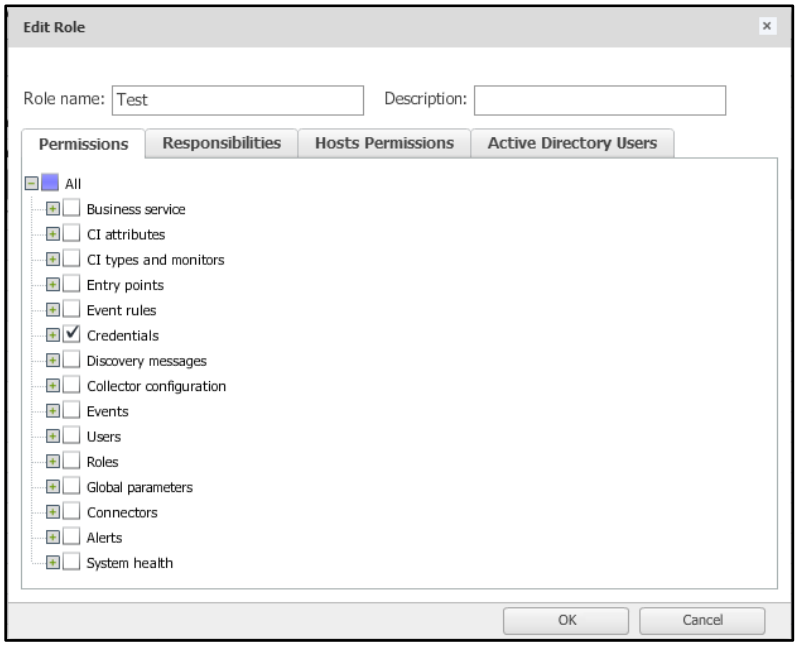
4. If you place the cursor over a **Permissions** or **Responsibilities** field, the entire content of that field Is displayed in a tooltip.





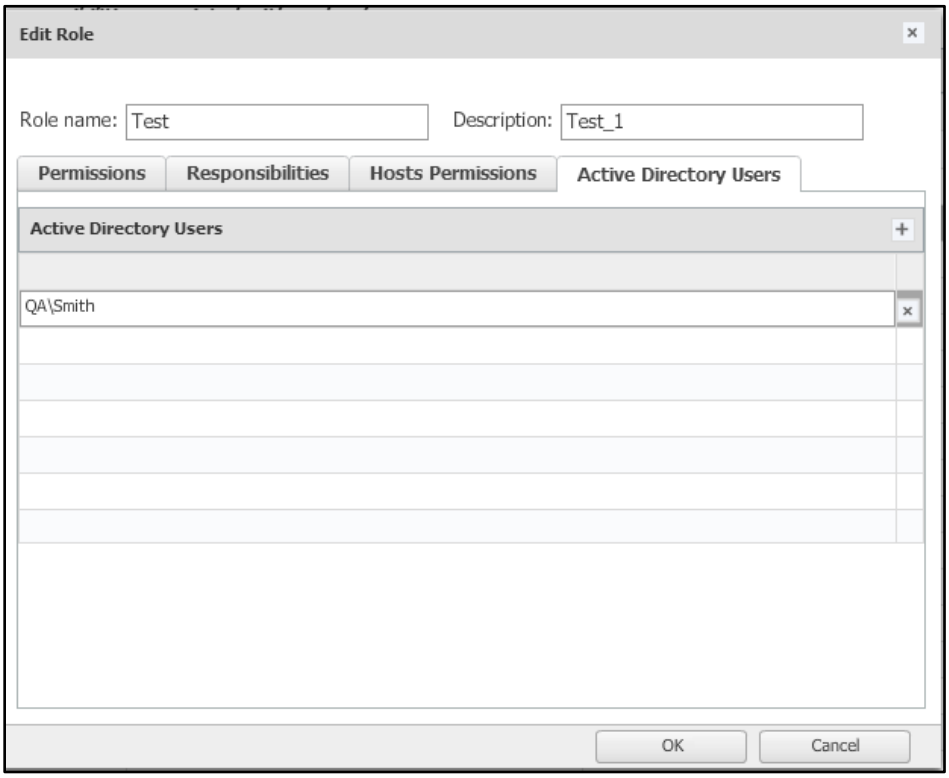
5. Double-click the required role (or first use the **+** button to add a new role and then double-click it). The **Edit Role** dialog box is displayed.

Figure 88: Edit Role dialog box



6. If applicable, select the Users, Roles, Global parameters and Discovery messages checkboxes.
7. Click the Active Directory Users tab. The Active Directory Users table is displayed.

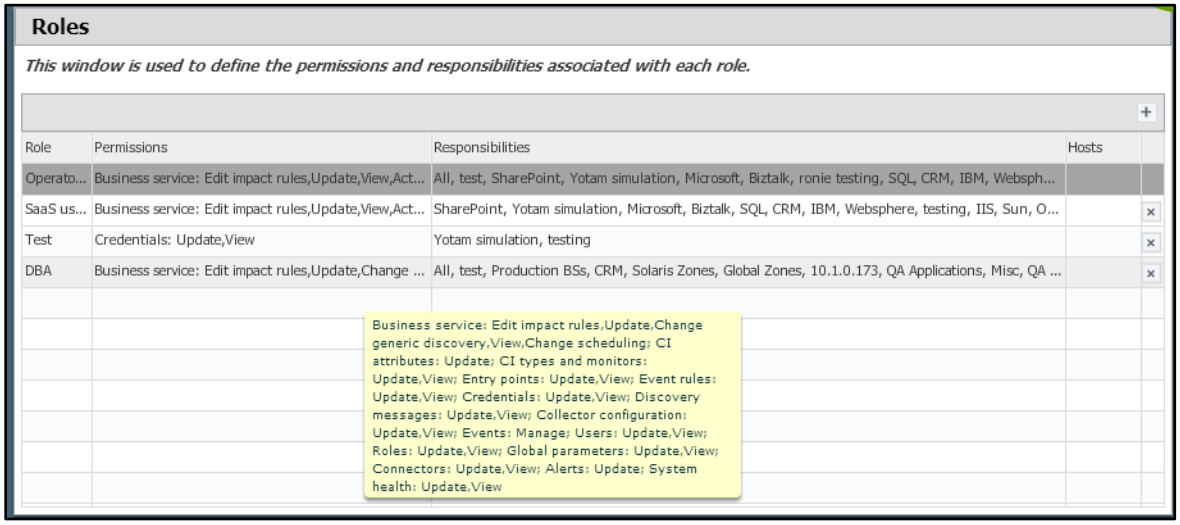
Figure 89: Edit Role dialog box – Active Directory Users panel



8. Click the **+** button to add **domain\user** names to the table. Then click OK.
   A **user** *without* a domain name (followed by a back-slash) cannot be added.

9. The list of domains should be configured in the **ad.properties** file which should be in the **ServiceWatch\server\conf\prop** directory. There are two formats for this list.
   - <domain name>=ldaps://<ip address:port> for example, qa=ldaps://10.1.0.1:636
   - <domain name>=ldap://<ip address:port> for example, qa=ldap://10.1.4.31:389
10. Use this panel or the **Active Role** window to list the authorized **Active Directory Users**.

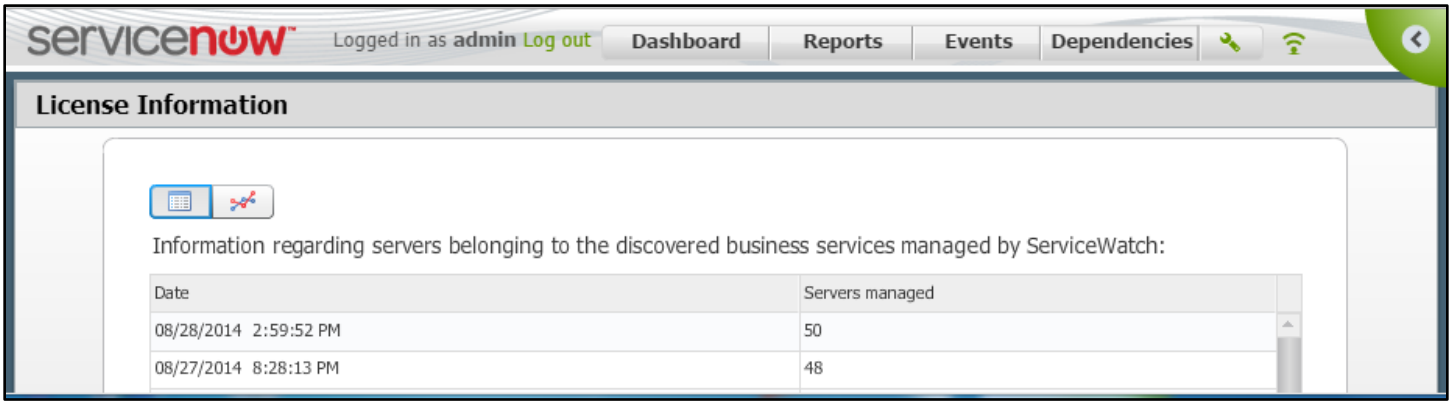
Figure 90: Role window after adding the DBA role



License Information

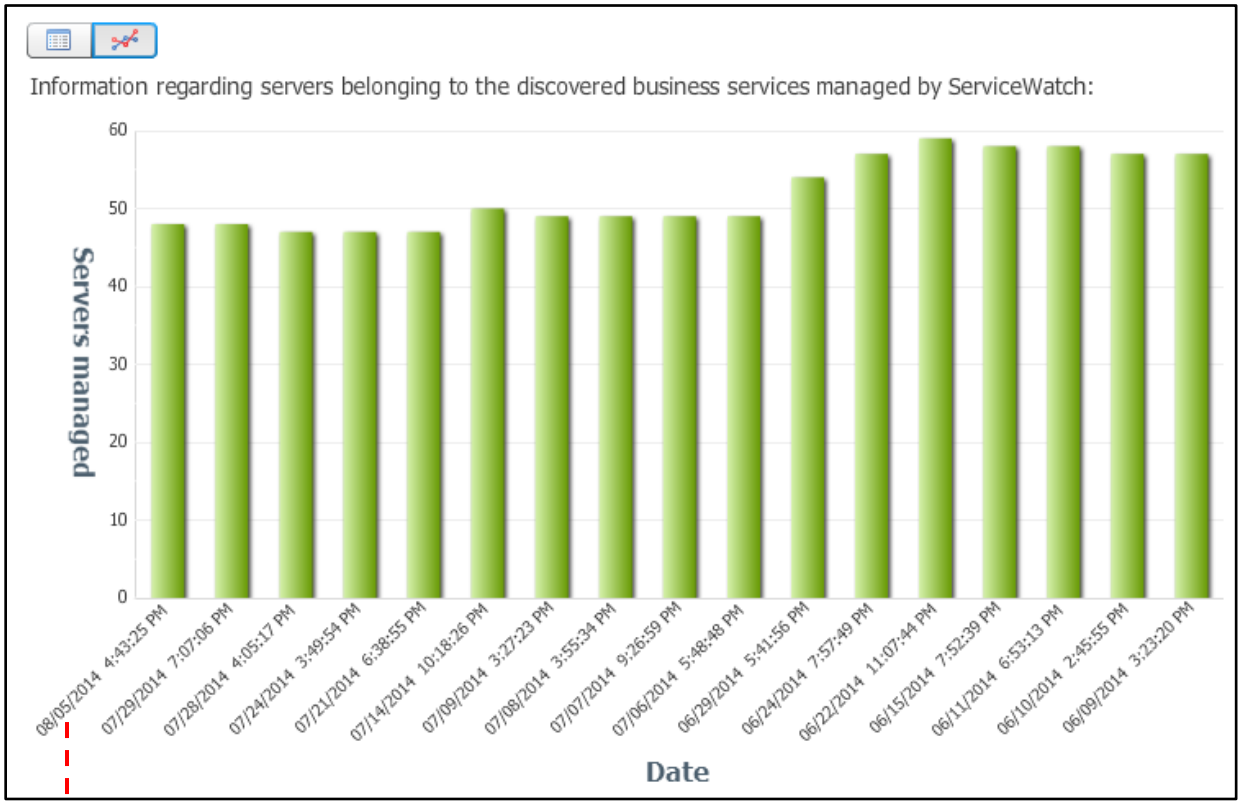
Click the **License Information** link in the **Settings** menu (Figure 64) to display the **License information** window. This window indicates the number of hosts that were part of the business services on the dates they were discovered. Click the left half of the  icon to display this data as a table.

Figure 91: License Information table



Click the right half of the  toggle icon to display this data as a graph.

Figure 92: License Information bar graph



When the cursor hovers over any bar of this graph, data about that bar is displayed in a tooltip.

User Management settings

Note: Before defining users, define the roles that they can perform.

Roles

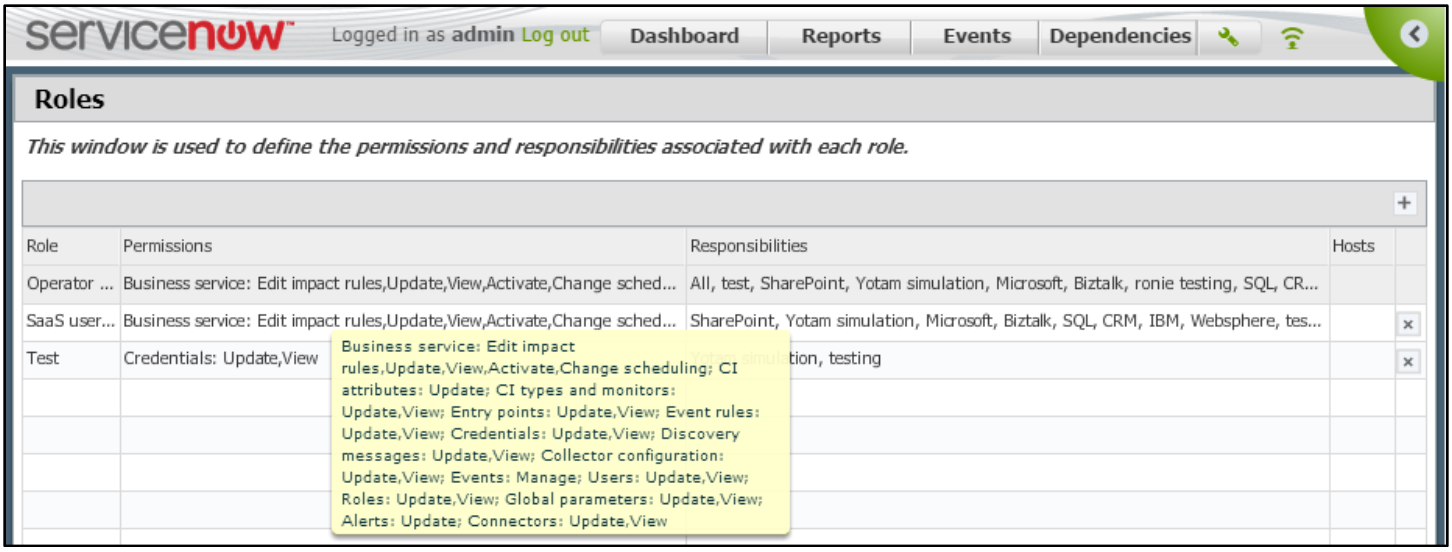
This window is used to define the permissions and responsibilities associated with each role. One or more roles are assigned to each user in the **Users** window.

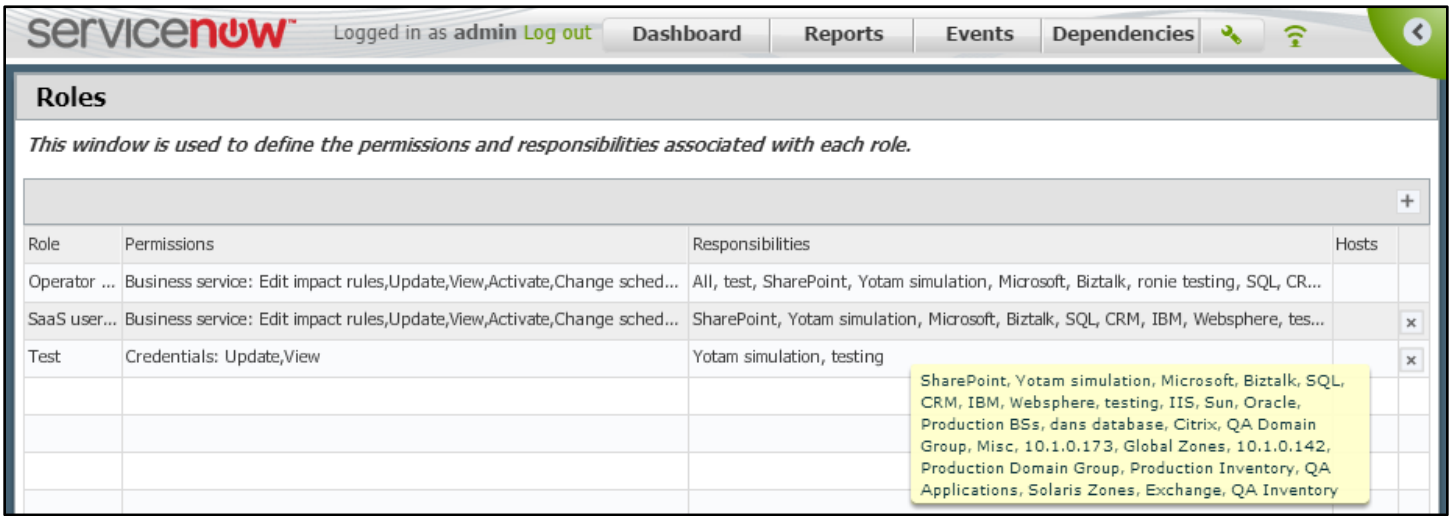
1. Click **Roles** in the **Settings** menu (Figure 64) to display the **Roles** window.

The complete entry for the **Permissions** and **Responsibilities** fields can be displayed in a tool tip.

The data can be sorted on the **Role** column by clicking the header of that column. Clicking that header again reverses the sort sequence.

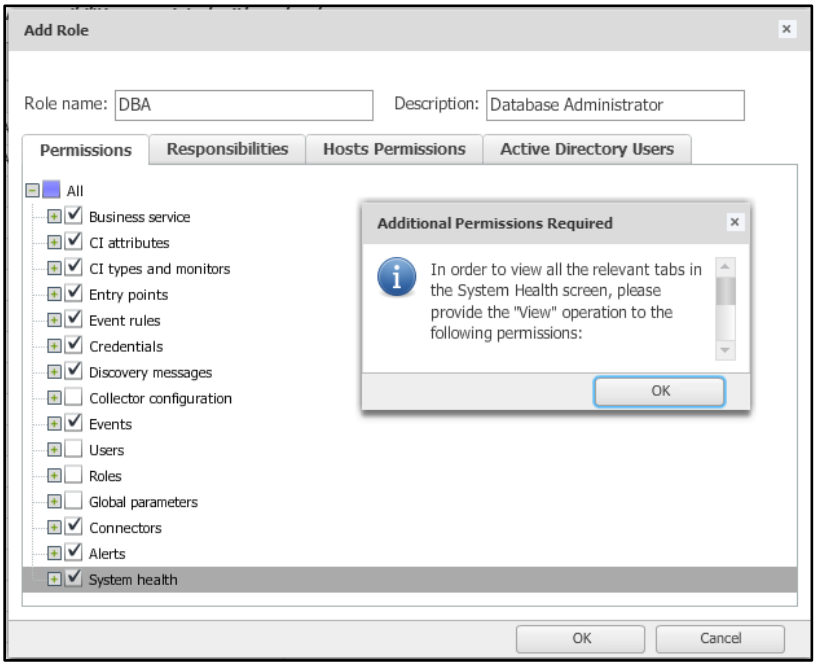
Figure 93: Roles windows with tool tips





2. Click the  icon in the blank header to add a new **Role. D**ouble-click an existing **Role** to edit it. The **Add Role** and **Edit Role** screens are essentially identical.

Figure 94: Add Role window with Permissions panel



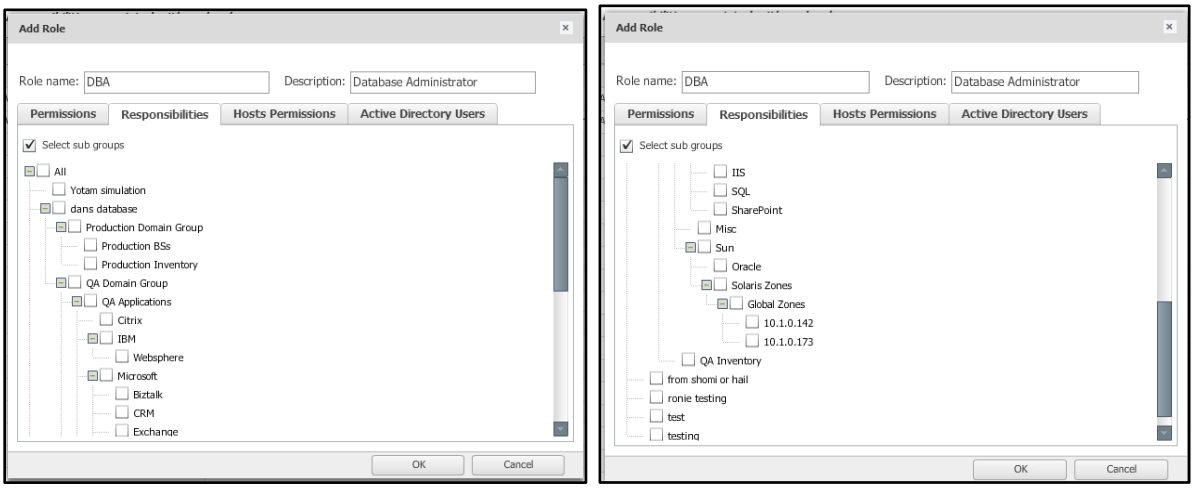
3. If the **Additional Permissions Required** message box is displayed, click its **OK** button after reading it.

Notes:

- ✓ Permissions are listed by object type. By expanding the object type, you can display actions that are relevant to the object type (for example, update, edit).
- ✓ To grant all permissions for an object type, select the checkbox for the object type.
  To grant specific permissions for an object type, expand the object type and select the checkboxes for the desired permissions.
- ✓ To grant all permissions for all objects, select the **All** checkbox.
- ✓ The Additional Permissions Required message indicates additional permissions that must be granted to fully use the requested permissions. For example, System Health permission requires Collector configuration permission.

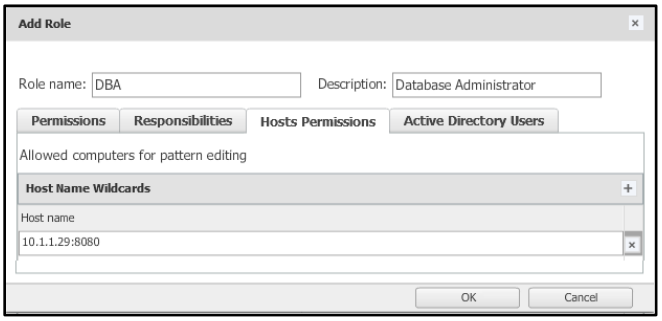
4. Click the Responsibilities tab to display a tree that lists business groups. You can expand or collapse the tree. Select the checkbox of the business services or business groups that the role can impact. Select the **All** checkbox to allow this role to apply to every business service.

Figure 95: Add Role window with Responsibilities panel



5. To grant permission to define discovery pattern editing on selected hosts, click the Hosts Permissions tab. The **Host Permissions** panel is displayed.

Figure 96: Add Role window with Host Permissions panel



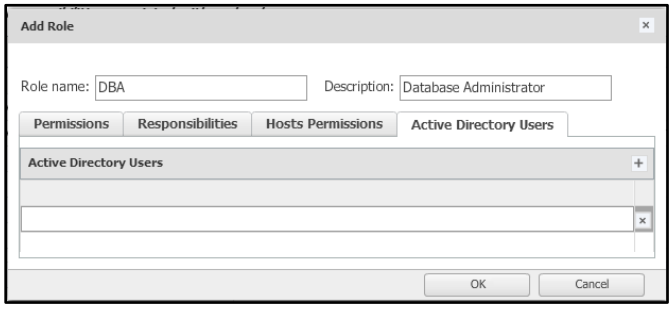
a. Specify the New host or IP wildcard.

b. To transfer the data to the Host/IP wildcards list, click the + button.

c. Repeat steps **a** and **b** for each new host or IP wildcard.

d. To delete an existing host or IP wildcard, click the × button on its row.

6. To add, modify or view **Active Directory Users**, click the **Active Directory Users** tab. The format for Active Directory Users is **domain\user** or LDAP distinguished name.

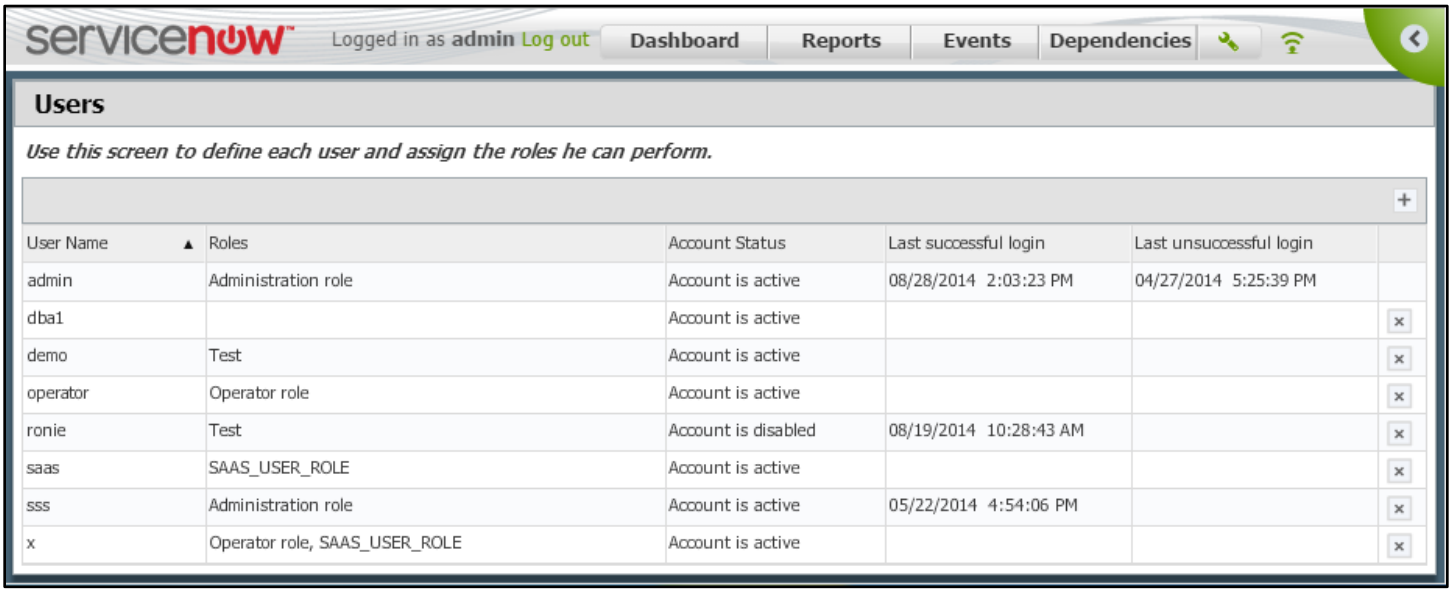


7. Click OK to save the specified data. Click Cancel to exit without saving data.

Users

Use this window to define each user and assign the roles he can perform. Click **Users** in the **Settings** menu (Figure 64) to display the **Users** window.

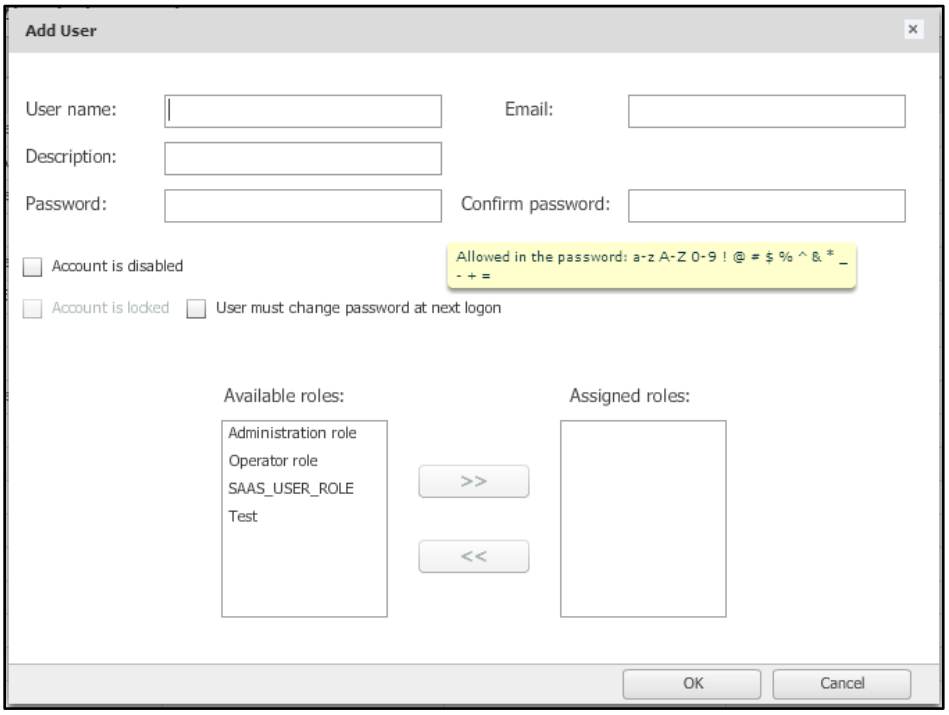
Figure 97: Users window



Click any column header to sort by that column. Click the same column again to reverse the sort order.

Click the + icon in the blank header row to display the **Add User** dialog box or double-click the row of an existing user to display the **Edit User** dialog box.

Figure 98: Add User dialog box



Enter the requested data in the text boxes.

Note: A **User Name** is limited to lower case letters, numbers, and a forward slash (to separate user and domain names). Upper case letters automatically convert to lower case.

To assign an **Available role**, highlight the role and click 

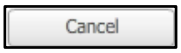
.

To delete an **Assigned role**, highlight the role and click 

.

To save the data and exit the dialog box, click 

.

To exit the dialog box without saving any data, click 

.

System settings

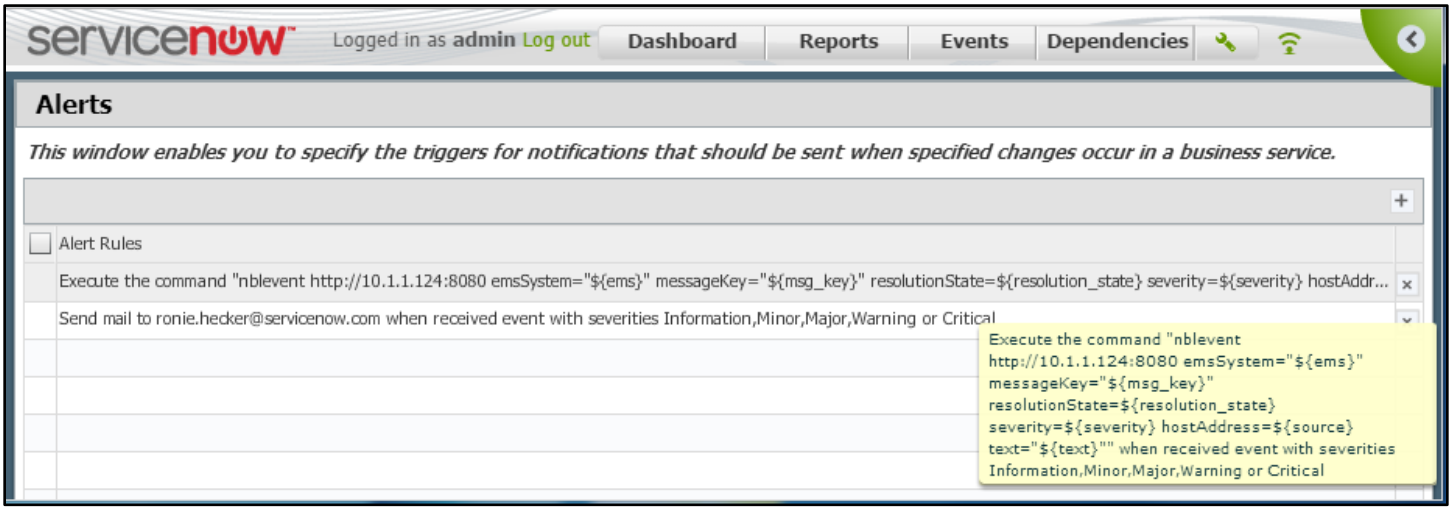
Alerts

Use this window to specify notices to be triggered when events or changes occur in a business service. Alerts can be triggered by a combination of:

- Events affecting specified CI types and the Severity level of CIs of those types.
- Changes in the Severity level of specified business services
- Topology changes that affect specified CI types belonging to specified business services

Click the **Alerts** link in the **System** area of the **Settings** menu to display **Alert Rules** in the **Alerts** window.

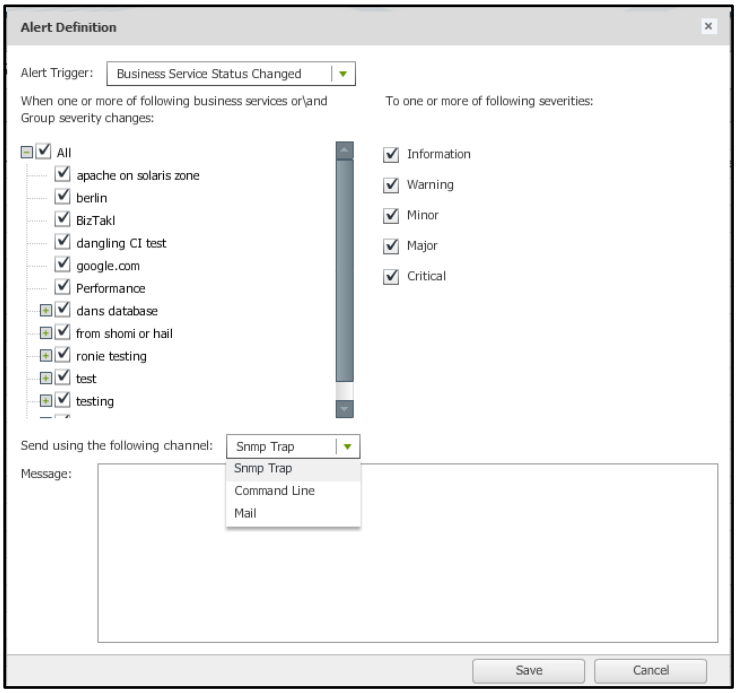
Figure 99: Alerts window

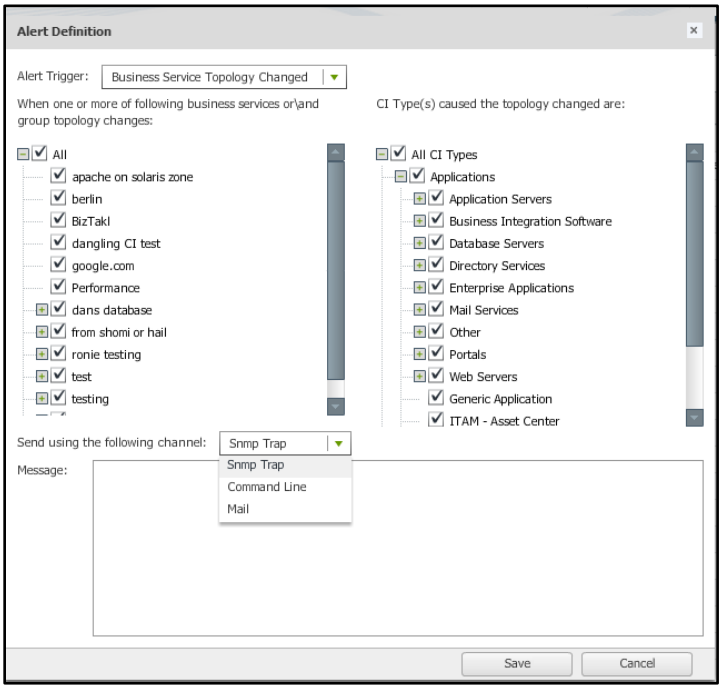


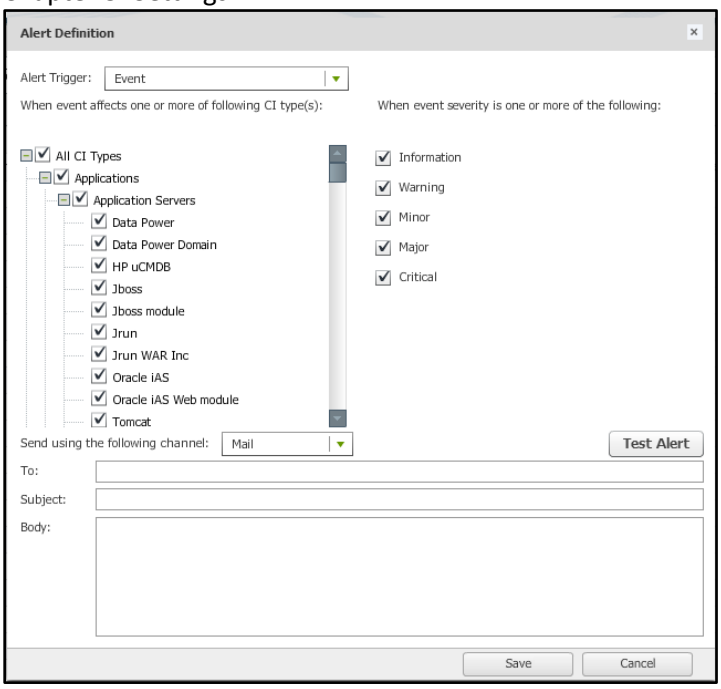
To add an alert rule, click [+] in the top right corner of the **Alert Rules** table header.
To edit an existing alert, double-click that alert in the **Alert Rules** table.
The **Alert Definition** dialog is displayed. It has 3 variations determined by the **Alert Trigger** value:

Click the **Alert Trigger** **green** down-arrow to select the type of trigger. One of these three dialog boxes is displayed.

Figure 100: Alert Definition dialog boxes (3 types)







Click  next to **All** or **All CI Types** to expand its tree. Select the **Business Services** and **Severities**, or the **Business Services** and **CI Types**, or the **CI Types** and **Severities** that should act as a trigger.

Then, click the **Channel** down-arrow to select a media for the alert: **Snmp Trap**, **Command Line** or **Mail**.

Finally, specify the Snmp Trap **Message**, or the Command Line **Command**, or the **To** (recipient), **Subject** (topic) and **Body** (message) for Mail.

For the **Command Line** and **Mail** channels, click 

to determine if the message can be triggered and received.

Click 

to add the new definition to the **Alert Rules** table. Click 

to exit the dialog box without saving the data.

Collectors

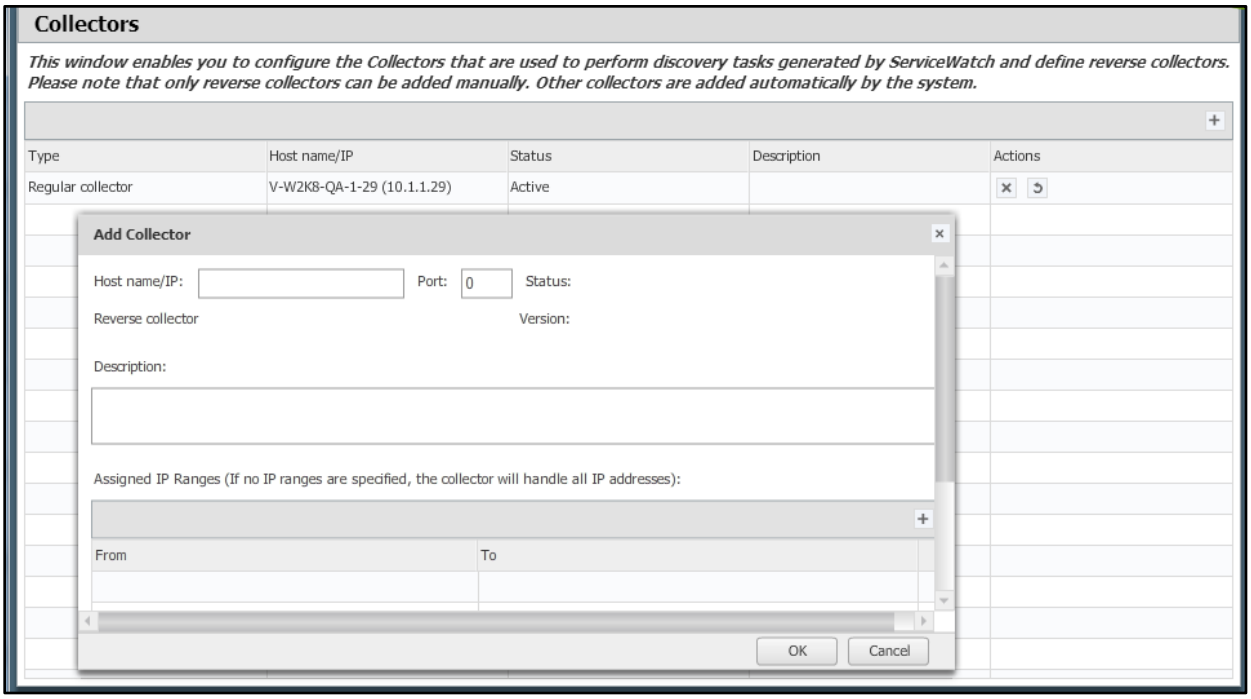
The ServiceWatch architecture consists of one Server plus one or more Collectors.

Regular Collectors receive discovery tasks from the Server, perform these tasks periodically, and automatically send the results to the Server.

Reverse Collectors perform discovery tasks only when requested to do so by the Server. Server-Reverse Collector communication is initiated by the Server instead of by the Collector

The Collectors window enables you to add, delete, configure, display, and activate/deactivate these Collectors. Click the **Collectors** link in the **Settings** menu (Figure 64) to display the **Collectors** window.

Figure 101: Collectors window with Add Collector dialog box



Because standard collectors are added automatically to the **Collectors** window, the **Add Collector** dialog box is used primarily to register **Reverse collectors**.

Adding a Collector

To display the **Add Collector** dialog box, click the + icon in the untitled header near the top right corner of the **Collectors** window. Fill in its fields and click OK to save the data on the next row of the **Collectors** window.

Deleting a Collector

To unregister a collector and delete it from the table of collectors, click the × icon in the **Actions** column on the row of that collector. The collector remains installed in the system but it is deleted from the **Collectors** screen and communication with it is terminated. If an unregistered standard collector (not a Reverse collector) is active, it should eventually re-register itself automatically and reappear in the **Collectors** window.

Activating a Collector

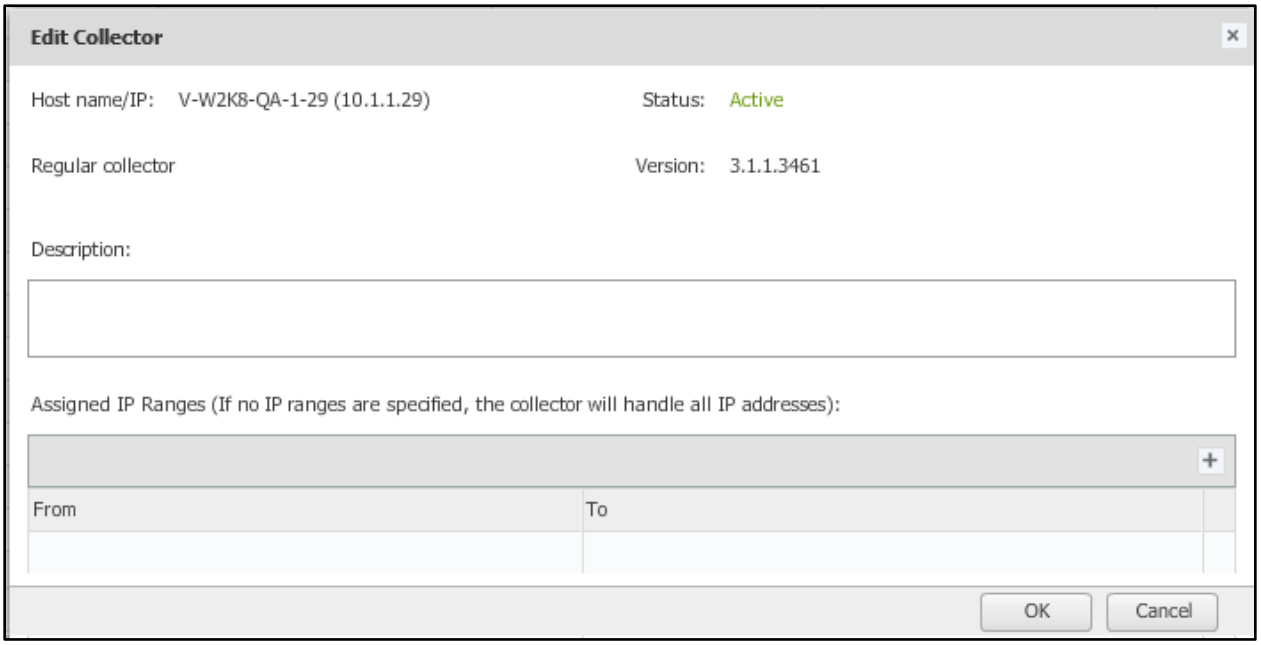
To restart a listed collector, click the icon in the **Actions** column on the row of that collector.

Editing a Collector

Collectors can handle different IP address ranges. These ranges can be specified in the **Edit Collector** dialog box. You can manually limit the network segments each collector handles by specifying the start and end of its IP range(s).

1. For each collector to be edited, perform steps 2 - 4.
2. Place the pencil cursor over any text field of the row to be edited and double-click. The **Edit Collector** dialog box is displayed (Figure 102).

Figure 102: Edit Collector dialog box



3. Optionally, specify a **Description** for the collector.
4. For each IP Range the collector handles, click + in the top right corner of the **From – To** table and use the pencil cursor to specify **From** and **To** IP values.
5. When you finish defining the ranges for the collector, click OK or Cancel to exit without saving changes.

Credentials

The **Credentials** window enables you to define the credentials that ServiceWatch needs to communicate with remote hosts during the discovery process. After you finish the ServiceWatch installation and configuration, you should supply the credentials that ServiceWatch needs to discover configuration items in your network.

Notes:

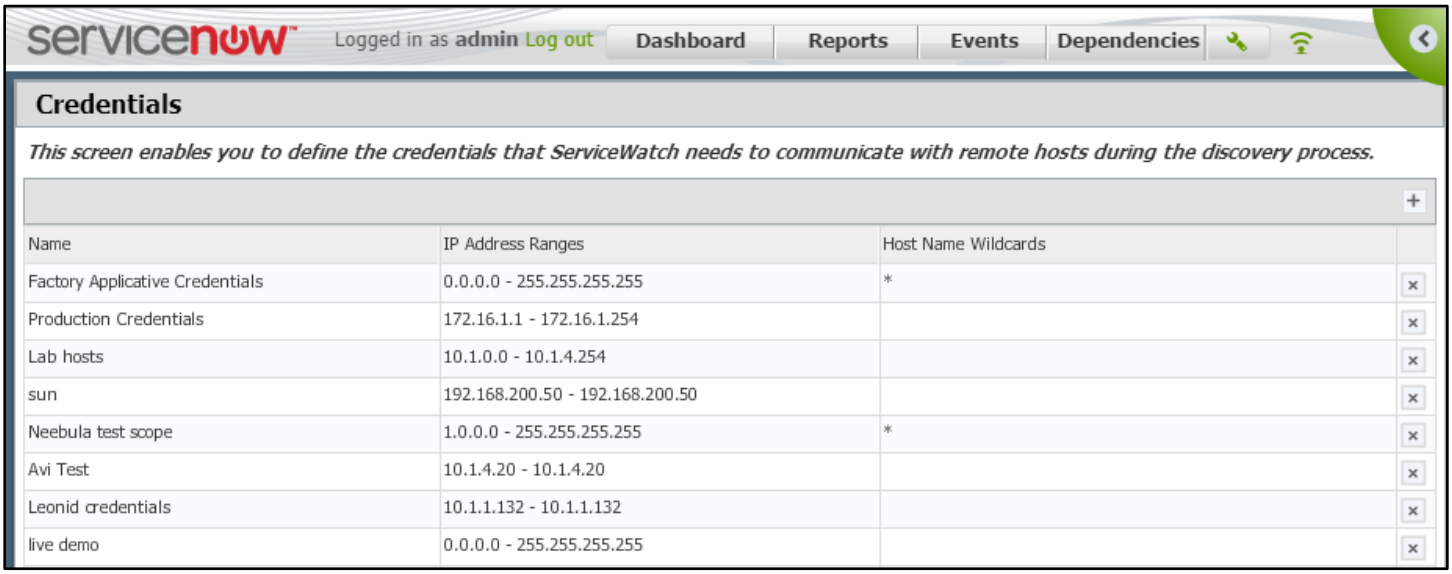
- The discovery credentials you supply are encrypted.
- If you forget to supply needed credentials when you configure a business service, you can supply those credentials when you adjust the business service topology as described in Adjusting the Business Service Topology.

Credentials are defined in the form of credential sets. A credential set consists of:

- Name of the credential set.
- Scope – Relevant machines specified as any combination of IP Address ranges and/or hostnames with wildcards. At least one IP address range or hostname must be specified.
- Credential type – Possible Credential types: Windows, Applicative, SNMP, LDAP, NetApp. The Applicative credential type is used for discovering an application or for using an application to discover a connection.
- Credentials – The actual credentials required vary by type. If the credential type is Applicative, you must also specify a CI type.

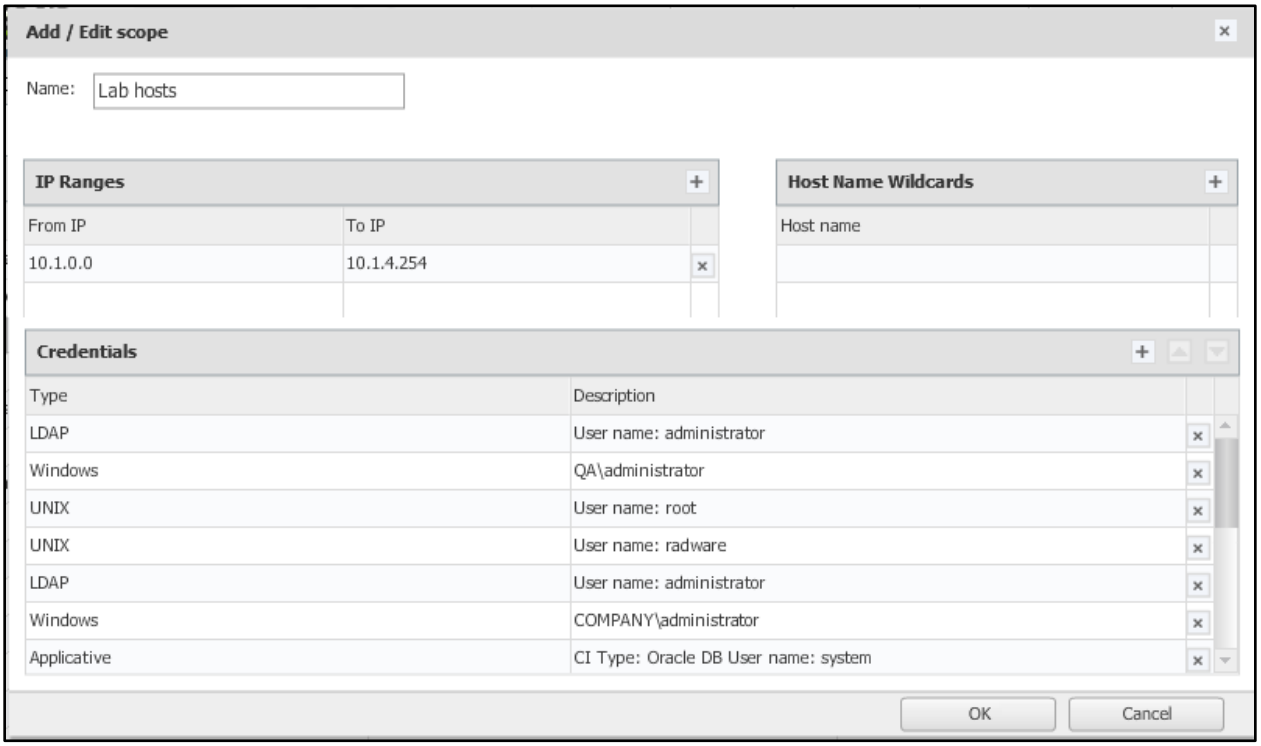
Clicking the **Credentials** link in the **Settings** menu (Figure 64) displays the **Credentials** window.

Figure 103: Credentials window



To add a new credential, click  in the header. To edit an existing credential, double-click any field in its row. In either case, the **Add / Edit scope** dialog box is displayed.

Figure 104: Credentials Add / Edit scope dialog box

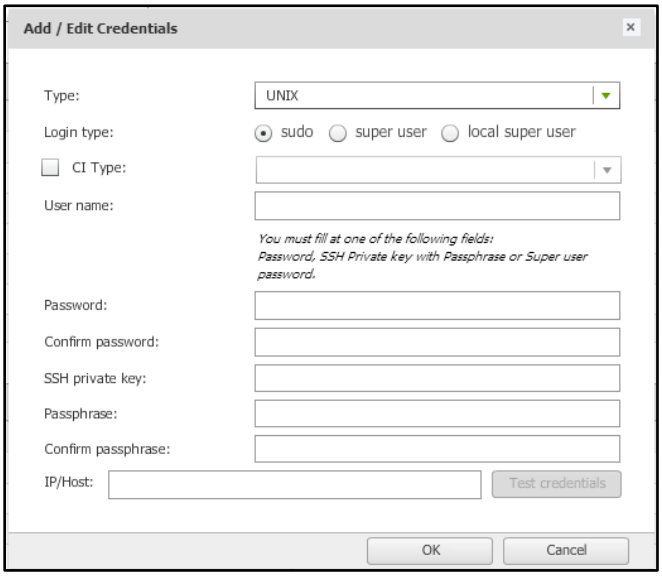


Note: The credentials you define are used in the vertical and network discovery processes to access all the machines that require credentials.

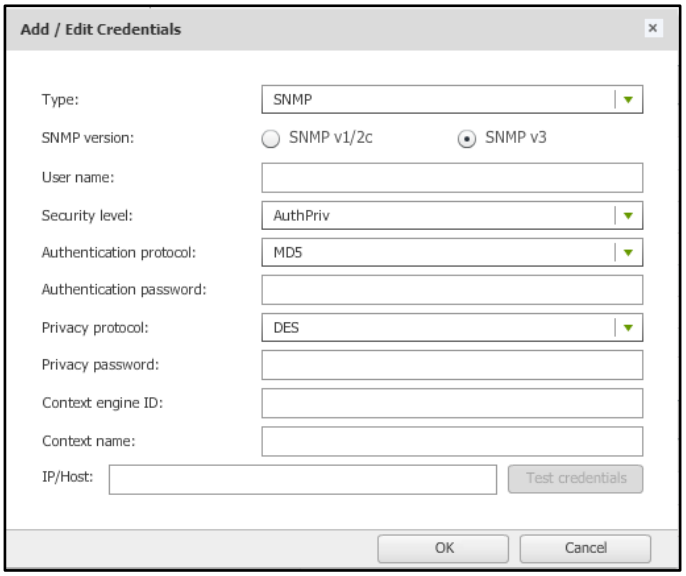
1. In the **Name** text box, specify a meaningful name for the credential set.
2. Click ⊞ in the **IP Ranges** header or double-click an existing row in that table.
3. Fill in or modify the **From IP** and **To IP** values.
4. Click ⊞ in the **Host Name Wildcards** header or double-click an existing row in that table.
5. Specify or modify the **Host name**. You can use the * wildcard (representing any number of characters) as a suffix or the full name.
6. Click ⊞ in the **Credentials** header or double-click an existing row to display an **Add / Edit Credentials** dialog box. The dialog box content is determined by the value in the **Type** field.

Figure 105: Add / Edit credentials dialog boxes

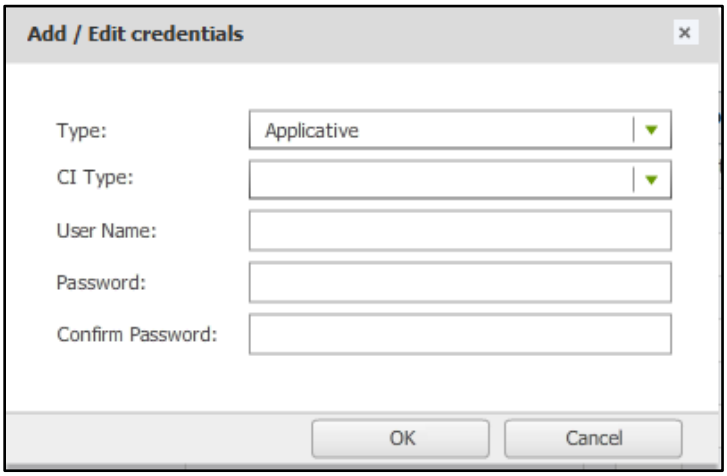
UNIX



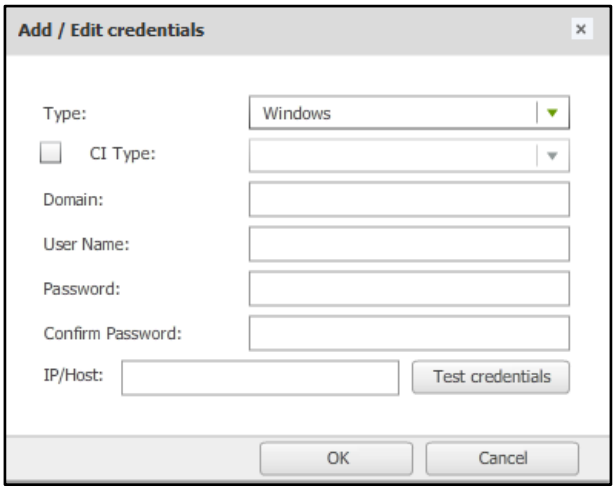
SNMP



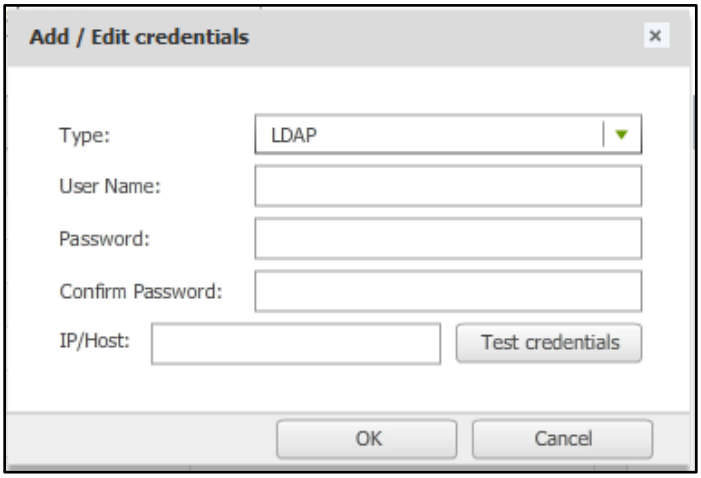
Applicative



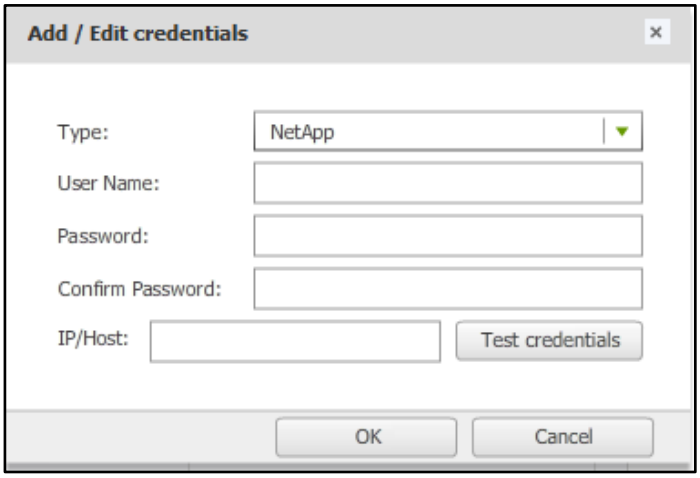
Windows



LDAP



NetApp



7. Define the credentials. To edit an existing value, click the relevant field and modify the value.
   a. Select the credential **Type** from the drop-down list. The fields displayed in the dialog box vary based on the credential **Type**.
   b. Fill in the dialog box fields. If you select **Applicative** as the credential **Type**, select the desired (configuration item) **CI Type** from the drop-down list and then fill in the credentials.
   c. If you select **SMNP** as the credential **Type** and the **SNMP v1/2c** radio button, only the **Community** and **IP/Host** fields are displayed. If you select the **SNMP v3** radio button, the SNMP fields shown in Figure 105 are displayed. Use the down-arrows to display possible values for the **Security level**, **Authentication protocol** and **Privacy protocol** fields that are not grayed-out. The **Context engine ID** and **Context name** fields are optional.

Note: Because SNMP v1/2c **community@vlan-id** and SNMP v3 **vlan-<vlan-id>** do not have the same format, the SNMP API must accept both formats and use the correct one.

   d. Click OK in the **Add/Edit credentials** dialog box or click Cancel to exit without saving data
   e. Repeat steps a - c for each Credential being added or edited in the set. {0.

8. When you finish defining each scope and the credentials in its dialog box(es), click OK in the **Add/Edit scope** dialog box.

Note: To delete an item or detail in any screen or dialog box, click the × icon next to the item or detail.

Figure 106: Add / Edit scope dialog box after adding one scope

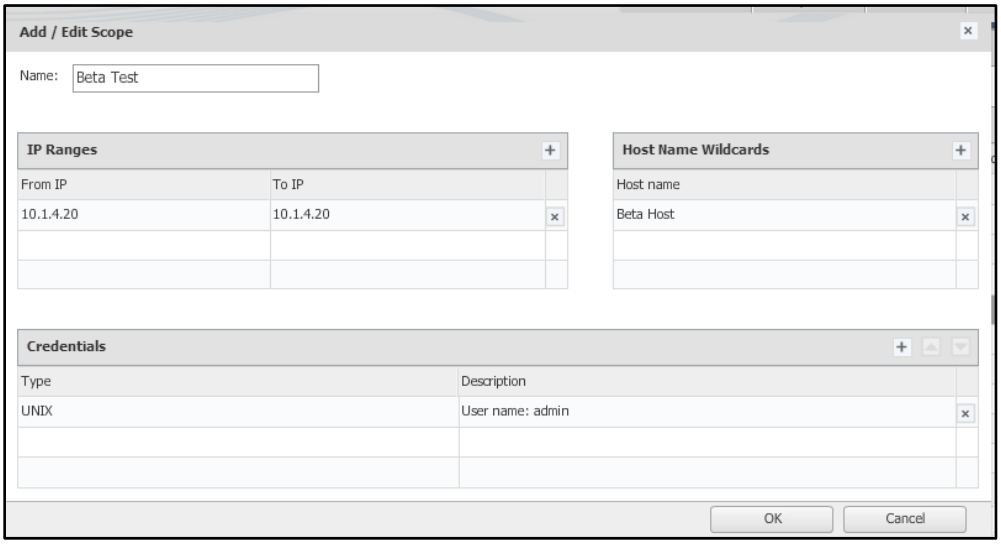
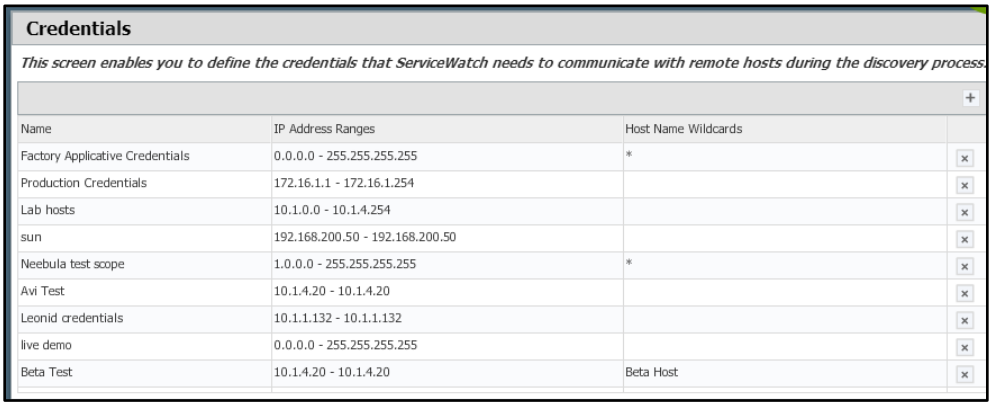


Figure 107: Credentials window after adding a Credential



Credentials

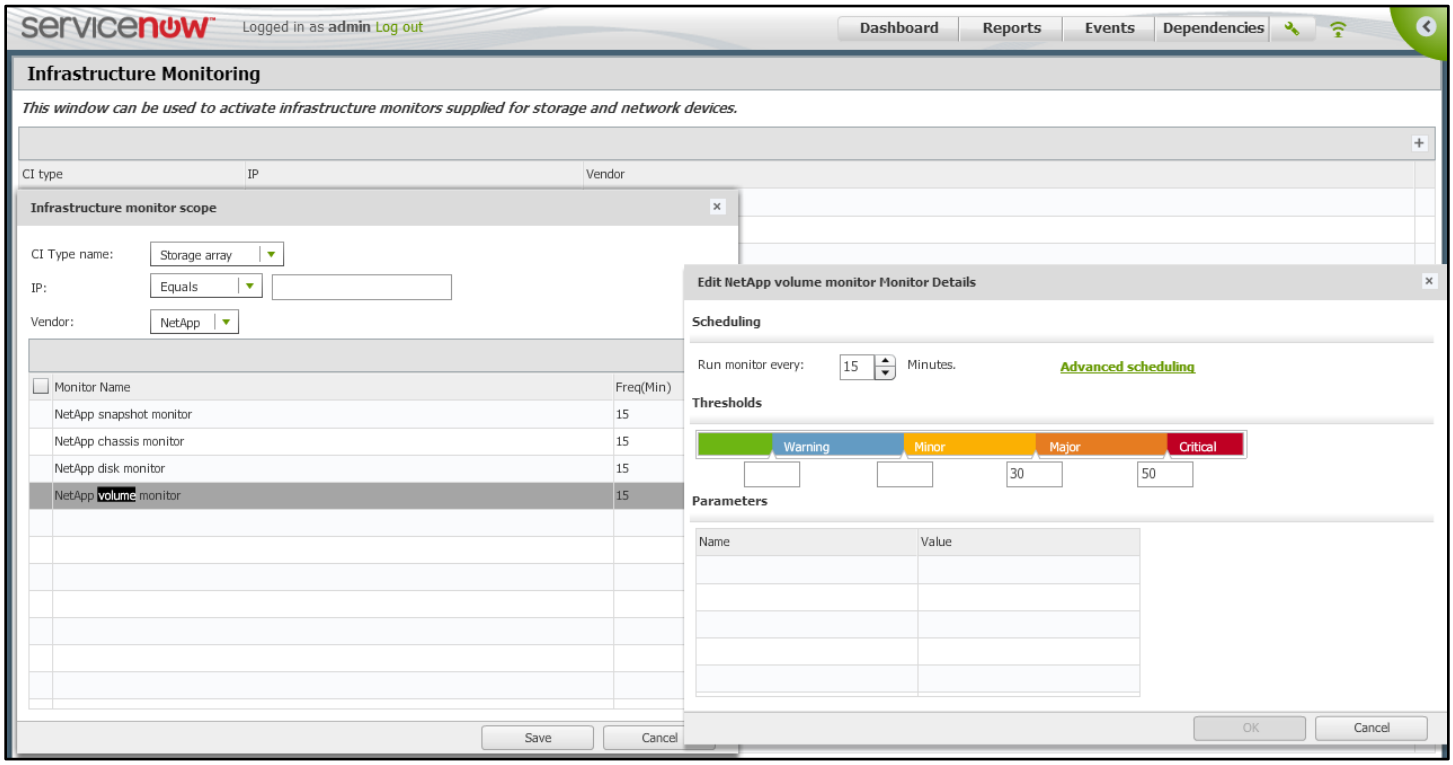
This screen enables you to define the credentials that ServiceWatch needs to communicate with remote hosts during the discovery process.

Name	IP Address Ranges	Host Name Wildcards
Factory Applicative Credentials	0.0.0.0 - 255.255.255.255	*
Production Credentials	172.16.1.1 - 172.16.1.254	
Lab hosts	10.1.0.0 - 10.1.4.254	
sun	192.168.200.50 - 192.168.200.50	
Neebula test scope	1.0.0.0 - 255.255.255.255	*
Avi Test	10.1.4.20 - 10.1.4.20	
Leonid credentials	10.1.1.132 - 10.1.1.132	
live demo	0.0.0.0 - 255.255.255.255	
Beta Test	10.1.4.20 - 10.1.4.20	Beta Host

Infrastructure Monitoring

This window can be used to create, edit and activate infrastructure monitors for storage and network devices. Click **Infrastructure monitoring** in the **Settings** menu (Figure 64) to display this window.

Figure 108: Monitoring screen with Monitor Scope & Monitor Details dialog boxes



Adding a Monitor

To add a monitor, click [+] in the top right corner of the **Infrastructure monitoring** table. In the **Infrastructure monitor scope** dialog box, use down-arrows to select **CI Type name** (e.g., Storage array), **Equals** an **IP** or **Between** an **IP range**, and the **Vendor** (e.g., NetApp). ServiceWatch handles **Network device** vendors such as 3Com, Brother Industries, D-Link Systems, F5 Labs and HP, and **Storage array** vendors such as **NetApp**.

Editing a Monitor

Display the monitor to be edited in the topology **Map**, select **Edit** mode, and click the **Monitors** tab in the bottom pane.

Double-click the **Monitor Name** to display the **Edit <Monitor name> Monitor Details** dialog box, select the frequency at which the monitor should run (in minutes), and specify **Event Severity** threshold values. To specify specific days and/or a specific time the monitor should run, click the **Advanced scheduling** link.

Click [OK] or [Cancel] to exit the **Edit <Monitor name> Monitor Details** dialog box.

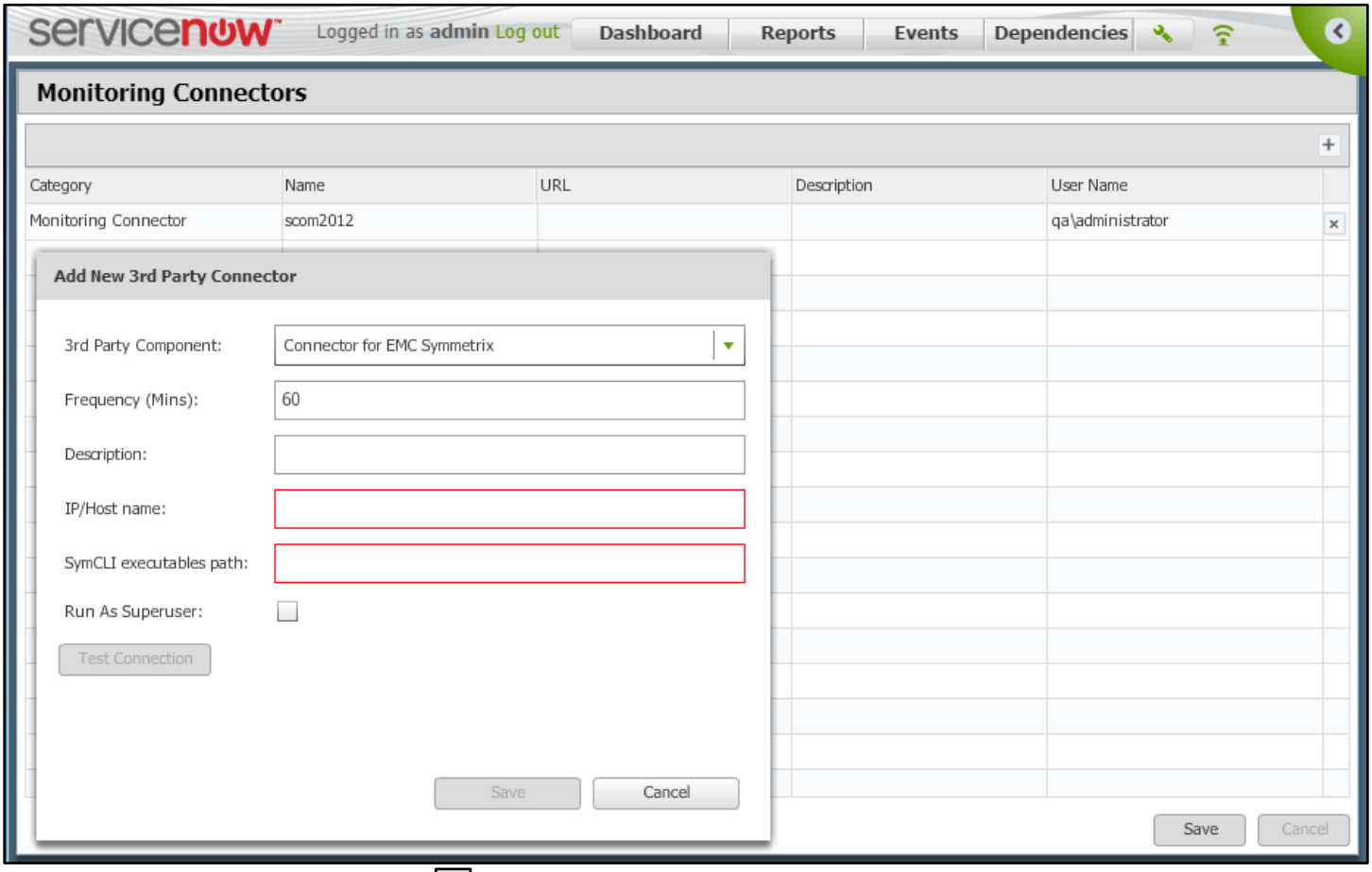
In the **Infrastructure monitor scope** dialog box, click [Cancel] to exit without saving or [Save] to add the new monitor data to the **Infrastructure monitoring** table.

Monitoring Connectors

This window specifies parameters that enable ServiceWatch obtain events from 3rd party monitoring systems that ServiceWatch recognizes, such as GroundWorks, IMAP, Netcool on Windows, POP3, and SolarWinds. For other monitoring systems via a command line or SNMP trap, contact ServiceWatch Customer Support.

Click the **Monitoring Connectors** link in the **Settings** menu (Figure 64) to display this window.

Figure 109: Monitoring Connectors window with an Add New 3rd Party Connector dialog box



To add a 3rd party connector, click [+] in the top right corner of the M**onitoring Connectors** table.

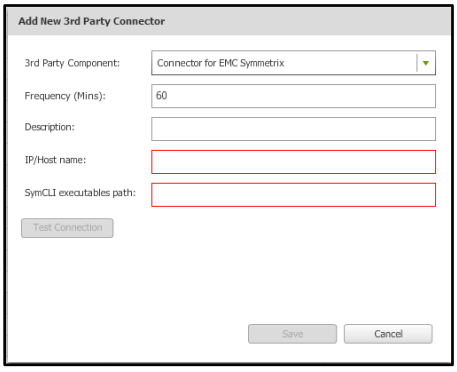
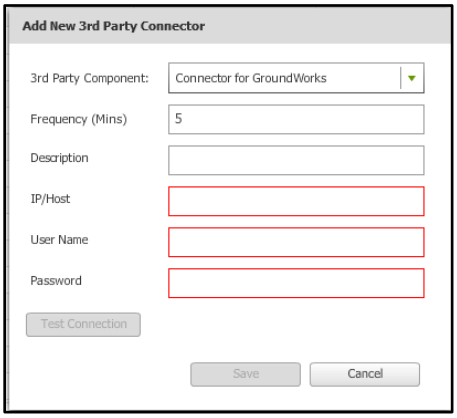
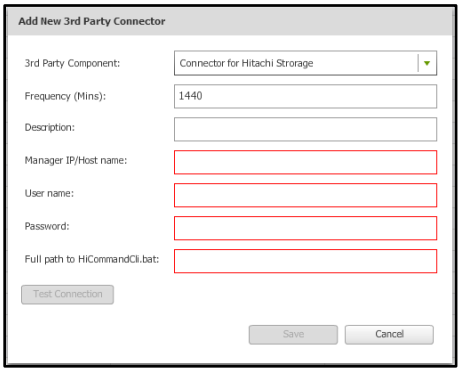
In the **Add New 3rd Party Connector** dialog box, use the down-arrow to select the **3rd Party Component** that is connected. ServiceWatch supports components such as: EMC Symmetrix, GroundWorks, HP EVA, IMAP, Netcool on Unix, Netcool on Windows, POP3, ServiceNow SolarWinds, Splunk, HP OpenView Unix, and Microsoft Operations Manager 2007. The EMC Symmetrix connector dialog box is illustrated above. Some other connector dialog boxes are illustrated below.

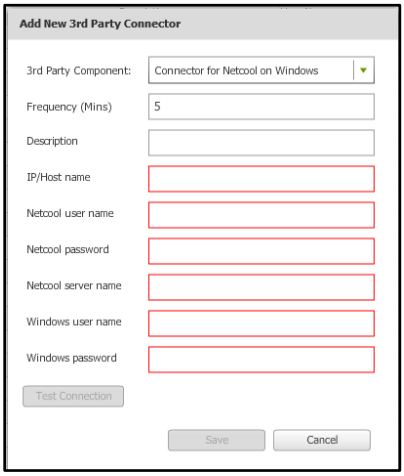
To modify an existing connector, double-click its row in the **Monitoring Connectors** table. The **Update 3rd Party Connector** window will be displayed.

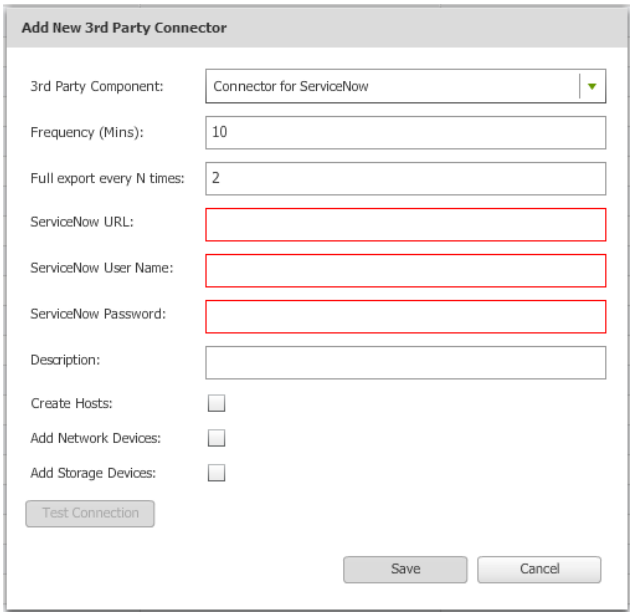
You can change the default **Frequency** and specify a meaningful **Description**. The remaining fields elicit data required to access the specified component.

Click [Test Connection]. If the test is successful, click [Save]. Otherwise, correct the values and test again or click [Cancel] to exit the dialog box without saving the data in it.

Figure 110: Add New 3rd Party Monitoring Connector dialog boxes – multiple types

	For information about monitoring EMC Symmetrix disk arrays, see http://sentrysoftware.com/kb/KB1052.asp
	GroundWork provides an open software platform for easy integration and customized visualization of cloud, virtualization, network, application, server, and storage data.
	For information about Hitachi Storage systems, see http://www.hds.com/products/storage-systems/ If using the Symantec NetBackup OpenStorage Connector, see http://www.hds.com/assets/pdf/hus-using-symantec-netbackup-openstorage-connector-for-hitachi-storage.pdf
	For information about the HP EVA component, see the HP EVA P6000 Storage data sheet.

	Internet Message Access Protocol (IMAP) allows an e-mail client to access e-mail on a remote mail server. IMAP servers usually listen on port 143. IMAP over SSL (IMAPS) is assigned port 993. IMAP supports on-line and off-line operations. E-mail clients using IMAP generally leave messages on the server until the user deletes them. Multiple clients can manage the same mailbox. Most e-mail clients support IMAP in addition to Post Office Protocol (POP).
	IBM Tivoli Netcool on Unix delivers near real-time, consolidated event management across business infrastructure, data centers, complex networks and IT domains. For data about setting Netcool environment variables for Linux and UNIX, use this link.
	For information about configuring IBM Tivoli Netcool on Windows, use this link.
	**Post Office Protocol** (**POP3**) is used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. Almost all e-mail clients and servers support POP3. Webmail service providers such as Google Mail, Microsoft Mail and Yahoo! Mail support IMAP and POP3.



This connector implements ServiceNow CMDB integration by enabling the export of ServiceWatch business service and CI data to analogous data in the ServiceNow CMDB.

The rate (in minutes) of the incremental export is configured via Frequency (Mins).

Every Nth incremental export is not an incremental export but a 'full export' that transfers data about all active business services.

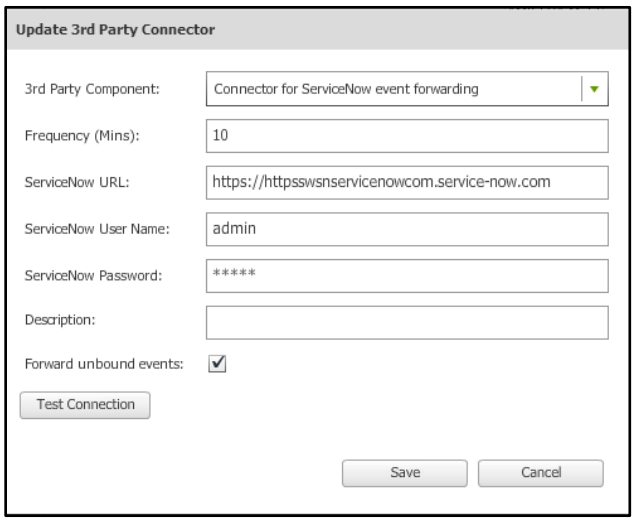
The **Full export every N times** field specifies the value for N.

The **ServiceNow URL**, **User Name** and **Password** are used to access the ServiceNow instance.

The **Description** of the ServiceNow instance is optional.

If **Create Hosts**, **Add Network Devices** or **Add Storage Devices** checkboxes are selected, ServiceWatch hosts, network devices and storage devices are also exported to the ServiceNow CMDB.

Note: After establishing a new connector, a Full export is performed.



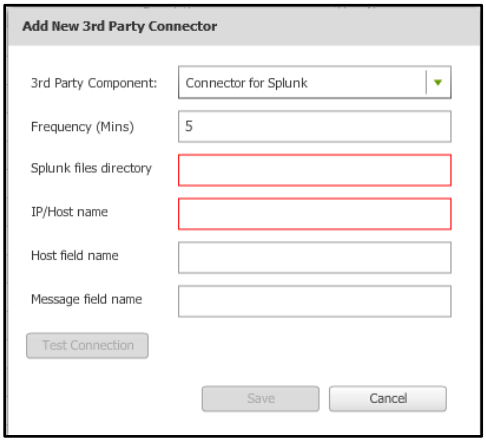
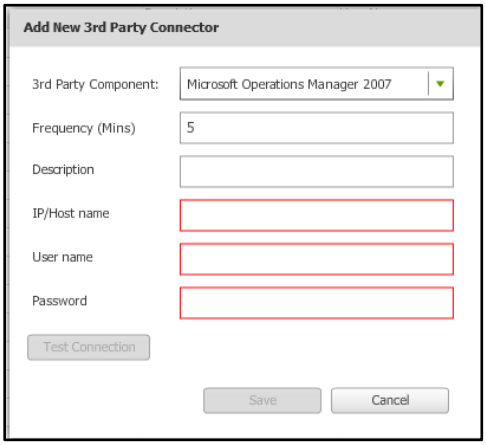
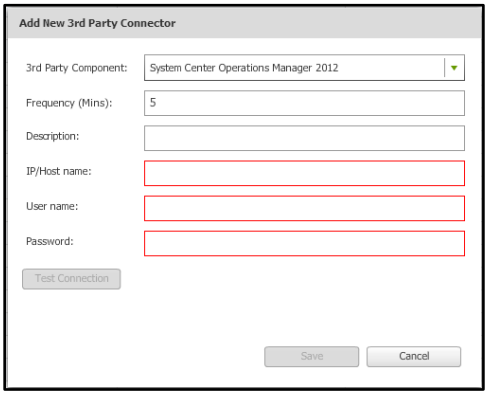
When defined, this connector automatically forwards active events (excluding acknowledgements) from ServiceWatch to the ServiceNow CMDB. When an event is closed in the ServiceWatch dashboard, it is also closed in the ServiceNow CMDB.

Unbound events are forwarded only if the **Forward unbound events** checkbox is selected.

The **Frequency** value specifies the time interval in minutes between each execution of the Event Forwarding connector.

The **ServiceNow URL**, **User Name** and **Password** are used to access the ServiceNow instance. The **Description** of the ServiceNow instance is optional.

SolarWinds Network Performance Monitor detects, diagnoses and resolves network performance problems and outages.

	Splunk Enterprise converts the machine data generated by IT systems and technology infrastructure into information about the status of computer networks and applications running on them.
	For information about integrating HP OpenView operations on UNIX, see this link.
	For information about System Center Operations Manager 2007, see http://www.networkworld.com/article/2230377/microsoft-subnet/understanding-how-system-center-operations-manager-works.html For data about System Center Operations Manager 2007, see http://technet.microsoft.com/en-us/library/bb310604.aspx
	For data about System Center Operations Manager 2012, see http://technet.microsoft.com/en-us/library/hh205987.aspx

Traffic Based Discovery

Discovery of CIs based on network traffic to or from them can be controlled at the global, business service, and individual CI levels.

- At the global level, use the **Traffic Based Discovery** parameters in Table 4: Global Parameters.
- At the Business Service level, display the topology in **Edit** mode, then click the **Definition** tab and the More details link at the bottom left corner of the **Definition** panel. In the **Traffic based discovery** field, use the down-arrow to select **True** (enabled) *or* **False** (disabled).
- At the CI level, select the CI in the **Map** panel in **Edit** mode, click the 

tab, and select the **Enable**, **Disable**, *or* **Same as business service** radio button.

If traffic based discovery is enabled at all levels and a topology Map becomes too cluttered with unneeded CIs at lower levels, you can use the following methods to reduce the clutter. In the **Edit** mode of the Map panel:

- Right-click a path under which you do not want to discover CIs and select the **Mark as Boundary** option.
- Right-click a CI of the type under which you do not want to discover other CIs and select the **Stop network based discovery from this CI Type** option.

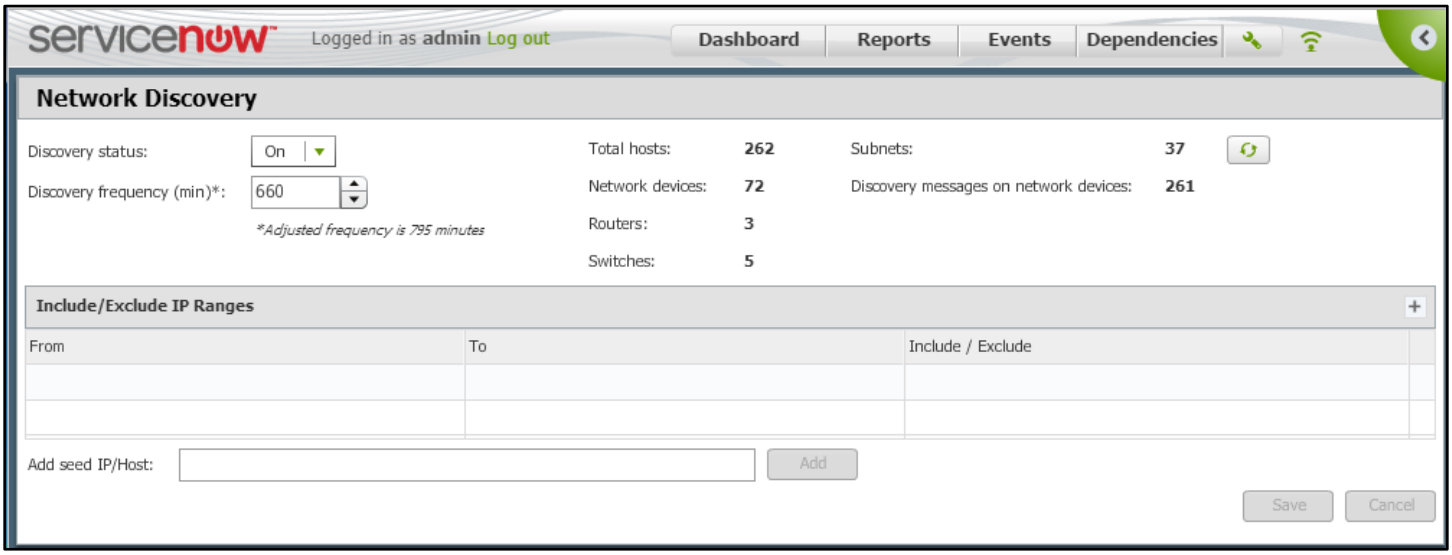
Network Discovery

It is important to define how often horizontal Network discovery should be performed and which IP ranges should be excluded. It is also necessary to identify as seed devices those network devices that ServiceWatch cannot recognize or identify. Network discovery tries to discover all devices in the network by using known devices as starting points but it can only do this from devices it can recognize or that are identified to it.

Note: ServiceWatch discovers and monitors the health of network paths based on the definitions you provide here. For information about viewing these network paths and displaying their health indicators, see CHAPTER 10: MONITORING NETWORKS.

1. In the **Systems** area of the **Settings** menu (Figure 64), select the **Network Discovery** option. The **Network Discovery** window is displayed.
2. Use the  button to refresh the data in this window.

Figure 111: Network Discovery window



3. From the **Discovery status** drop-down list, select **On**. Use the up and down arrows to set the **Discovery frequency** in minutes.
4. If IP ranges should be excluded from the discovery, specify those ranges as follows:
   a. Click  at the top right corner of the **Exclude the following ranges** table.
   b. In the activated text boxes, specify the **From** and **To** values for the IP range.
   c. Repeat steps **a** and **b** for each IP range to be excluded.
5. If the network discovery must pass through a physical device that is not seen (for example, a router), for each such device, specify the device in the **Add seed IP/Host** field and click its
6.  button. If you enter an invalid IP or Host, an error is displayed in the Network Discovery panel (see page 69).
7. When you finish defining the network criteria, click  .

System Health

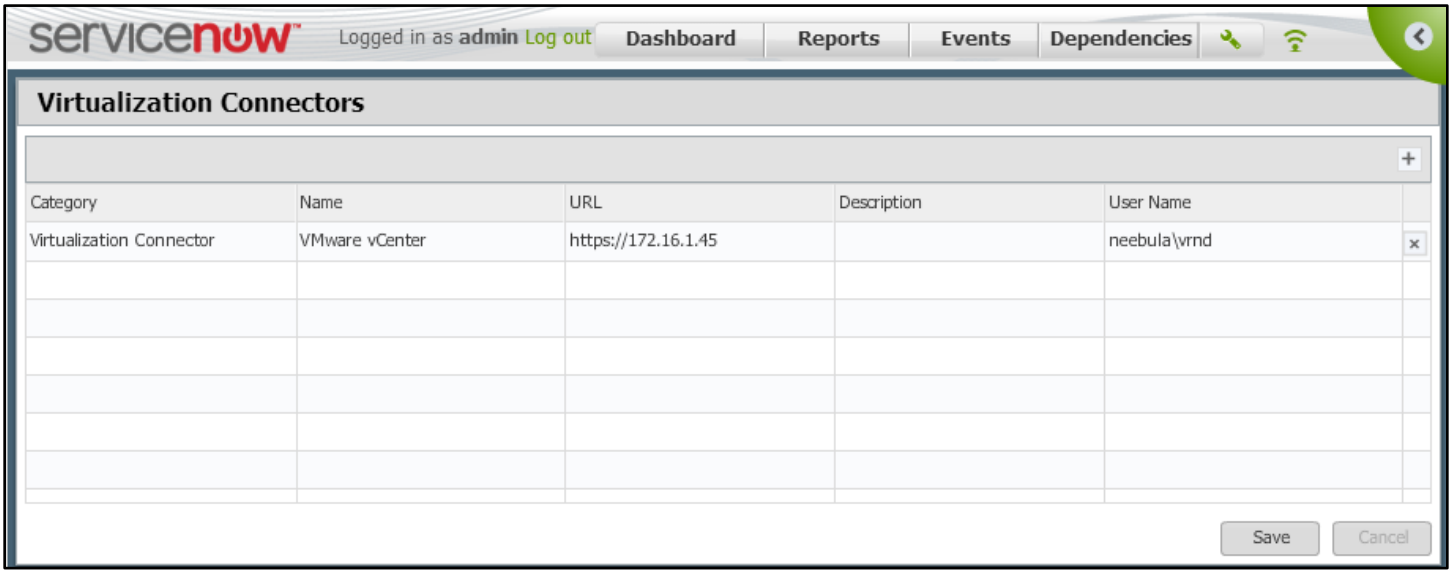
For a description of the **System Health** screen, see System Health on page 63.

Virtualization Connectors

Click the **Virtualization Connectors** link in the **Settings** menu (Figure 64) to display the **Virtualization Connectors** window. Use this window to obtain discovery information from these virtualization vendors:

- ✓ AMAZON_AWS – connects to an Amazon virtualization platform to discover virtual hosts (see https://aws.amazon.com/)
- ✓ ECC – connects to an ECC platform to discover EMC storage devices (see http://www.emc.com/?fromGlobalSiteSelect)
- ✓ vCenter – connects to a VMware virtualization platform to discover virtual hosts (see http://www.vmware.com/)
- ✓ Xen – connects to an Xen virtualization platform to discover virtual hosts (see http://xen.org/)

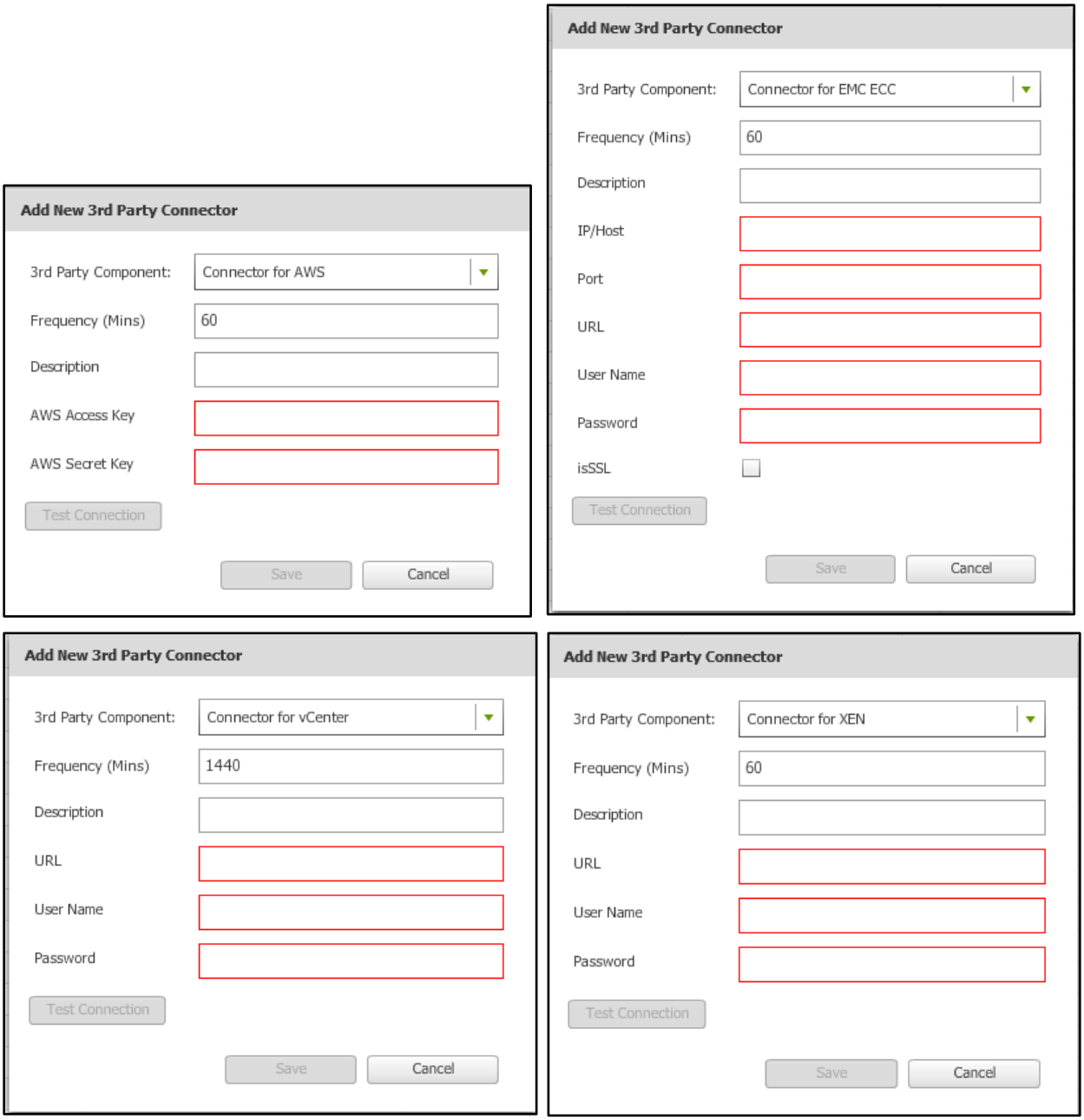
Figure 112: Virtualization Connectors window with Add New 3rd Party Connector dialog box



To add a new 3rd party Virtualization connector, click ⊞ in the top right corner of the **Virtualization Connectors** table. In the **Add New 3rd Party Connector** dialog box, use the down-arrow to select the virtualization vendor. The required fields will dynamically change based on vendor that is selected.

To update a Virtualization connector, double-click that connector's row in the **Virtualization Connectors** table.

Figure 113: Add New 3rd Party Virtualization Connector dialog boxes – 4 types



You can change the default **Frequency** (in minutes). Specify a meaningful **Description**. Other parameters vary depending on the virtualization vendor that was selected.

Click Test Connection. If the test is successful, click Save. Otherwise, correct the values and test again or click Cancel to exit the dialog box without saving the data in it.

Chapter 6: Configuring Business Services

This chapter contains the following topics

Note: This chapter deals with various aspects of discovery. For more information about this topic, see Appendix A: Discovery Workflows and the *ServiceWatch Customization Guide*.

Concepts

After installing and configuring the ServiceWatch server and collectors and after specifying credentials, the next task is creating and configuring groups, business services, and technical business services. Some of these tasks are performed manually; others automatically.

Groups are logical 'containers' that keep related business services together.

A technical business service is a collection of components that is treated as a business service even though it is not one. Unlike regular business services whose details are generated through discovery, technical business services are manually defined queries that facilitate the tracking of specific types of components. For example, every instance of a device type can be assigned to a technical business service monitored by a user who has expert knowledge of that device.

An *aggregate* monitor enables you to monitor the performance of a collection of CIs in a Group or a Business Service as a unit. It combines the results of similar monitors and enables you to view the combined output of those monitors. These monitors are described at Aggregate Monitors on page 187. KPIs produced by an aggregate monitor are called Aggregate KPIs.

Groups, business services and technical business services are created by right-clicking a node in the **Active** or **Pending** tree and selecting the appropriate option in the pop-up menu. Dialog boxes help you define and configure the group, business service or technical business service.

After a business service or technical business service has been activated, you can define a monitor for that service and specify its frequency of operation by clicking  , clicking the Group & Business Service Monitors option, right-clicking the service to be activated in the **Active** tree, and clicking **Add New Monitor** in the pop-up menu (see Chapter 8: Monitoring Business Services).

Entry Points Pane of the Definitions Panel

In this panel, you create a business service definition and specify its entry points. An entry point is a pointer to an application on a host. It is the starting point from which discovery is performed. Each business service must have at least one entry point. Different types of entry points can be used (for example, HTTP) and each type requires that appropriate values be specified for it (see Figure 116).

Topology Map

When you finish defining the entry points and click Save and view Map, ServiceWatch performs a top-down discovery from each defined entry point and displays a topology map of the objects in the business service. You can display the **Element Properties** of each object in the topology (Figure 147).

Ideally, the topology map should be error free and ready for use. However, sometimes adjustments are needed: For example:

- If Discovery cannot drill down below an object because of credential problems, it issues an error. You can either provide the needed credentials or mark the problematic object as a boundary to let the Discovery process know it should not try to drill down deeper.
- You may determine that a discovered object belongs to a different business service.
- You may want to exclude a discovered object from the topology even if it does belong to the business service.

After you are satisfied with the topology map, it is used for re-discovering active business services so that ServiceWatch is always using the most up-to-date topology.

In **Edit** mode, you can define the impact status of each object. For information about impact status, see DEFINING OBJECT IMPACTS ON THE BUSINESS SERVICE on page 133.

In **View** or **Edit** mode, you can display the properties of each object by clicking the **Properties** tab in the top right panel.

When you are satisfied with the topology, you can save it and activate the business service.

The Technical business service dialog box enables you to define one or more queries that select the components that belong to the technical business service. The Save and view Results button displays all devices that satisfy that query.

After you activate a business service and its monitors, ServiceWatch monitors it, updating its topology according to the frequency criteria you defined. After business services are created and configured, you can manage them from the **Monitoring** screen by selecting the appropriate node in the **Active** tree in the top left panel or the **Pending** (not active) tree in the bottom left panel.

Business Groups

You can use business groups to keep related business services together. When creating a new business service, you can assign it to a new or existing business group. You can also move or copy existing business services to a group.

Note: To place a business service in a group that does not yet exist, first create the group. To create a Technical Business Service, see Creating Technical Business Services on page 150.

While you are working in the topology screens, you can:

- Manipulate the topology map
- Collapse or expand groups in the topology displays
- Display business services in the Dashboard by selecting the **Active** root or by clicking the **Dashboard** button until the Dashboard is displayed
- Work on a different business service by selecting it in the **Active** tree

Creating and Configuring a New Business Service

To create and configure a new business service, perform the following steps:

1. Creating a New Business Service
2. Adjusting the Business Service Topology
3. Defining Object Impacts on the Business Service{0.

These steps are described below.

Notes: If you plan to place a business service in a group that does not yet exist, first create the group (see BUSINESS GROUPS on page 133).
To create a Technical Business Service, see CREATING TECHNICAL BUSINESS SERVICES on page 150.

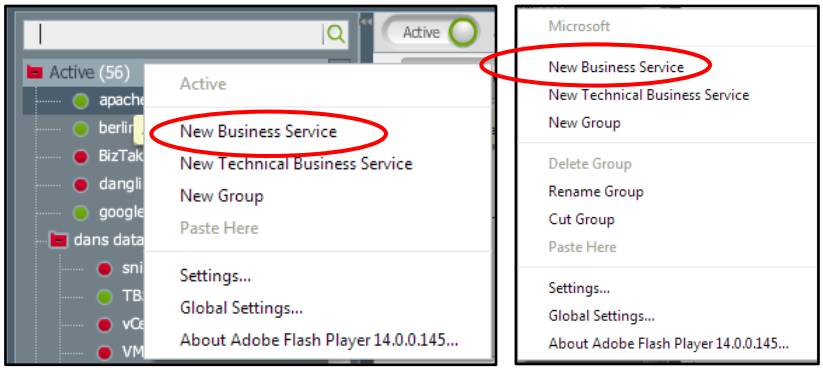
While you are working in the topology map screens, you can:

- Adjust the screen display. For details, see Adjusting the Topology Map on page 162.
- Collapse or expand groups in the topology displays
- Display business services in the Dashboard by selecting the Active root or by clicking the Dashboard button until the Dashboard is displayed.
- Work on a different business service by selecting it in the Active tree

Creating a New Business Service

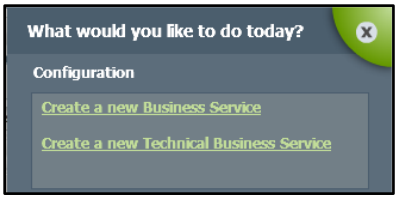
1. To create a new business service, select the node in the **Active** tree where you want to create it. To create the business service in a group, select the group. To create the business service at the root level, select the **Active** root. Then right-click the node, group or **Active** root and select **New Business Service** in the pop-up menu…

Figure 114: New Business Service option in pop-up menus



2. *or* click the **green** left-arrow icon in the top right corner  and select the **Create a new Business Service** link in the **What would you like to do today?** pop-up.

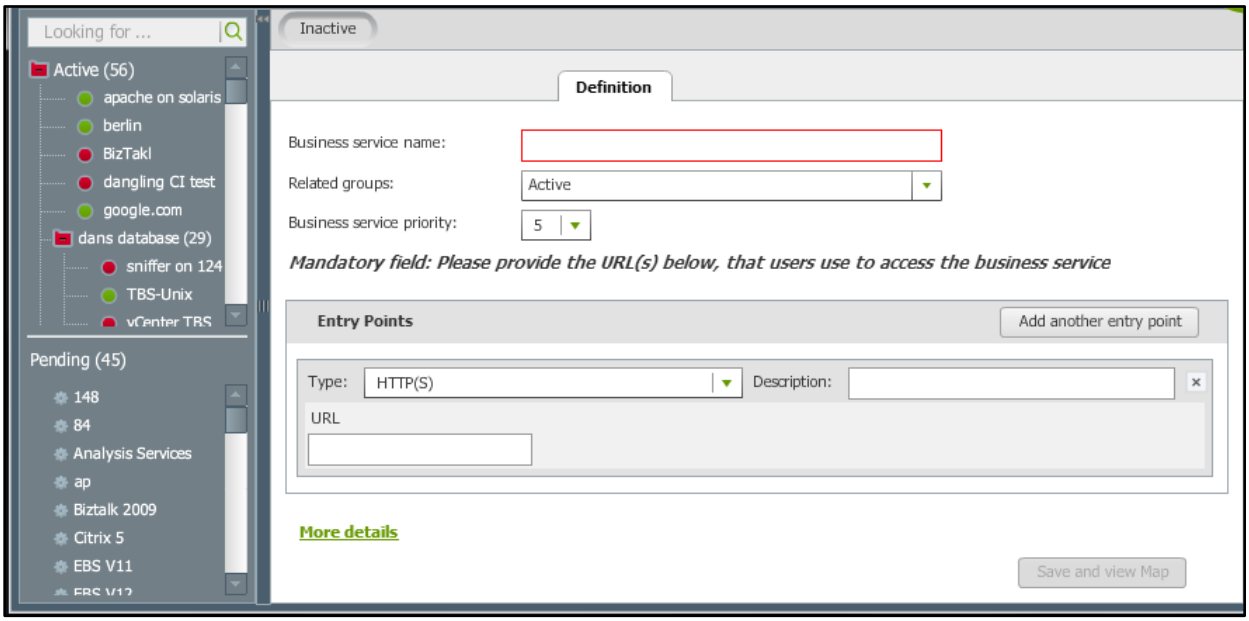
Figure 115: What would you like to do today? Pop-up menu



Defining Entry Points

3. The Definition and Entry Points screen of the Business Service wizard (Figure 116) is displayed.

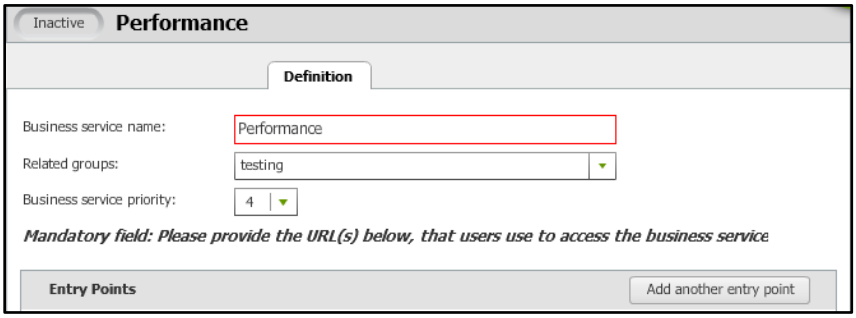
Figure 116: Definition panel and Entry Points pane of the Business Service wizard



a. Fill in the **Business service name.** As you type each letter, it is displayed in the header.

b. Click the **Related groups** down-arrow and select or uncheck the checkbox of each group.
In this example, the **testing** group has been selected. You can retype the **Business service name** and use the **Related groups** down-arrow to change checkbox selections.

Figure 117: Definition panel of the Business Service wizard



c. Use the **Business service priority** down-arrow to specify a value from **1** = lowest to **5** = highest. {0.

4. Specify the Type, Description and URL for one or more Entry points:

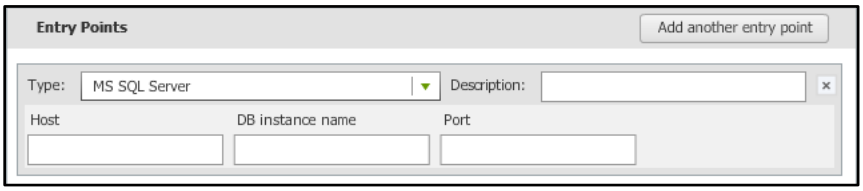
Figure 118: Business Service wizard Entry points pane with URL field

a. Select the entry point **Type** from its drop-down list.

b. Specify a meaningful **Description** for the entry point.

c. Specify the other fields for this Entry point. The displayed fields change according to the **Type** selected. For example:

Figure 119: Entry points pane with Host, DB instance name & Port fields



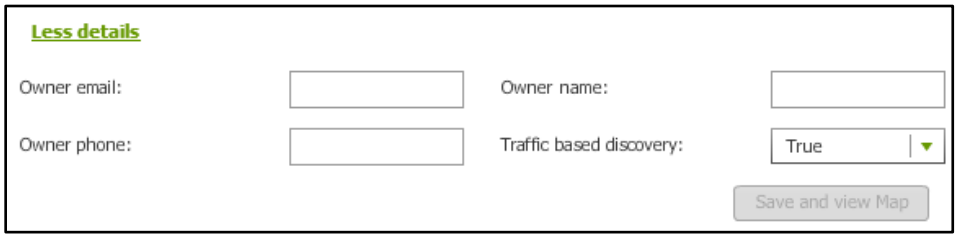
d. For each additional entry point, click 

and repeat steps a, b and c.

5. To specify an optional Owner name, phone, email address, Customers who use this business service, and/or to specify whether Traffic based discovery is (true) or is not (false) used, click the More details link. To hide these fields, click the Less details link.

Note: These attributes are configurable.

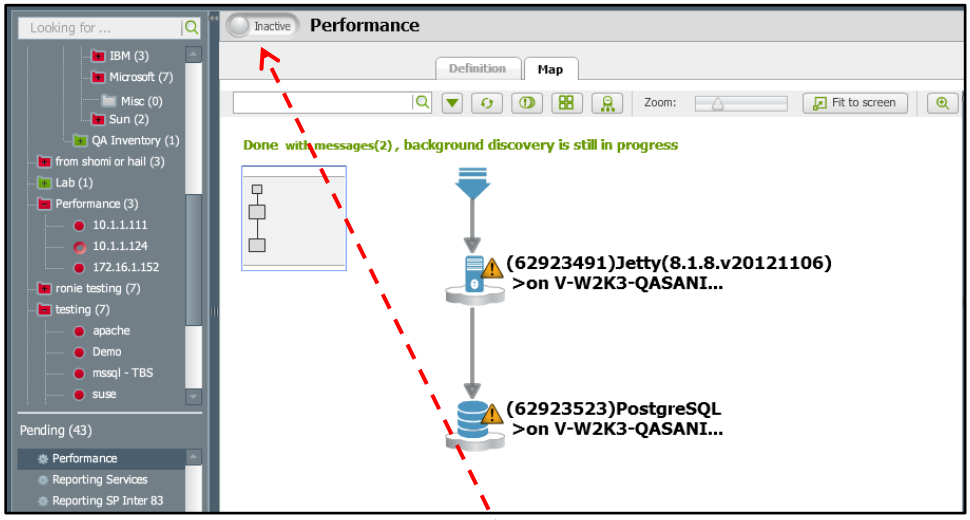
Figure 120: Business Service wizard More details fields



6. When you finish defining entry points, click 

to invoke the Discovery process and then generate and display the topology **Map** of the new Business Service (Figure 121). As the Discovery process progresses, discovered objects are displayed in the panel. The default state of each new business service is **Inactive** and it is listed in the **Pending** panel on the Dashboard.

Figure 121: Business Service Topology panel



7. To activate this business service, click 

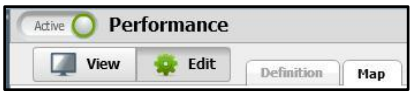
in the top left corner. The business service's state indicator will change to 

and it will move from the **Pending** panel to the **Active** tree. To disable this business service, click 

. The business service's state indicator will change to 

and it will move from the **Active** tree to the **Pending** panel.

8. When the business service is 

, the **View/Edit** 

toggle buttons are displayed. Click **View** to view the topology **Map**.

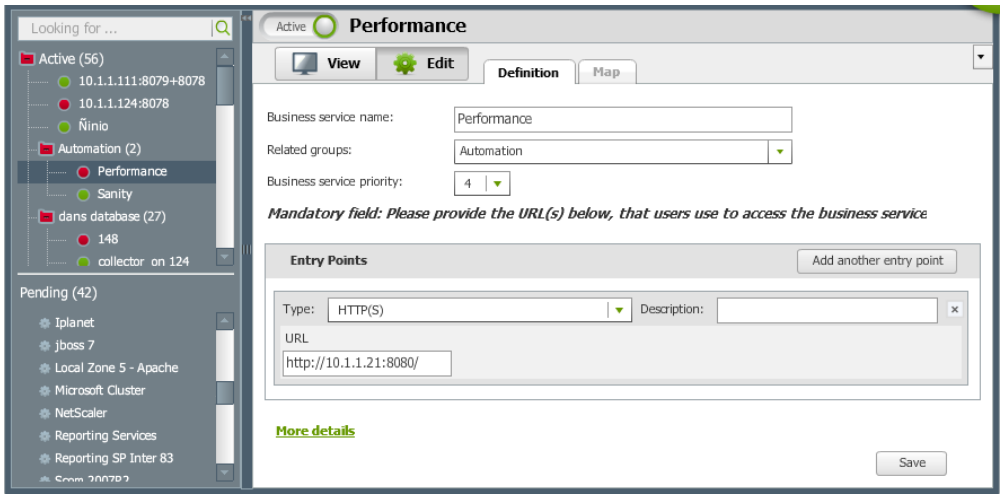
Performing Manual Operations

1. When the business service is 

, the **View/Edit** 

toggle buttons are displayed. Click **Edit** to edit the **Definition** or the topology **Map**.

Figure 122: Business Service Definition panel in Edit mode



2. If you modify the business service definition *without* changing **Entry points** data, a 

button lets you save the changes without invoking the Discovery process. If you do change **Entry points** data, the 

button invokes the Discovery process and redisplays the topology **Map**.

Notes:

- Hold the cursor over an object to display additional information about the object.
- You can display the Element properties of any object in the topology. For instructions, see Business Service, Object or Connection.
- You can display a Network Path for the connection between two objects. For information about this topic, see CHAPTER 10: MONITORING NETWORKS.
- The  icon in a topology map indicates a manually added boundary that inhibits discovery. See Table 5: Topology Map Adjustment Options for Objects on page 140.

Adjusting the topology map

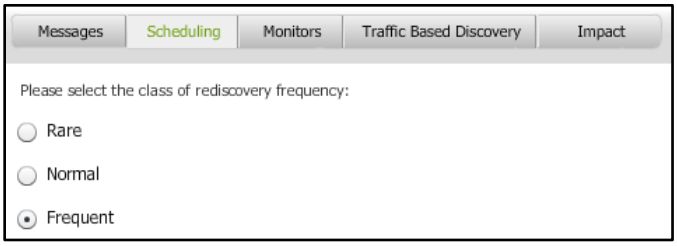
3. If adjustments to the topology map are needed (for example, the map contains errors), perform the adjustments. For instructions, see Adjusting the Business Service Topology.

Defining Status Impact Rules

4. For an explanation of object impact rules and instructions for defining them by status, see DEFINING OBJECT IMPACTS ON THE BUSINESS SERVICE on page 141. Click any object in the topology to display its impact rules.

Discovery Scheduling

Define Discovery Schedules

1. For each object in the topology, define how often discovery should be performed as follows:
   a. While in the **Edit** mode of the **Map** panel, select the object. If it is a cluster, click the empty space in the cluster box.
   b. Click the **Scheduling** tab in the bottom pane.
   c. 

   d. Select the radio button that indicates how often discovery should be performed for the selected object. Valid values:
      - Rare – Every 12 hours
      - Normal – Every hour
      - Frequent – Every 15 minutes
   e. The selected discovery interval is saved automatically.

Adjusting the Business Service Topology

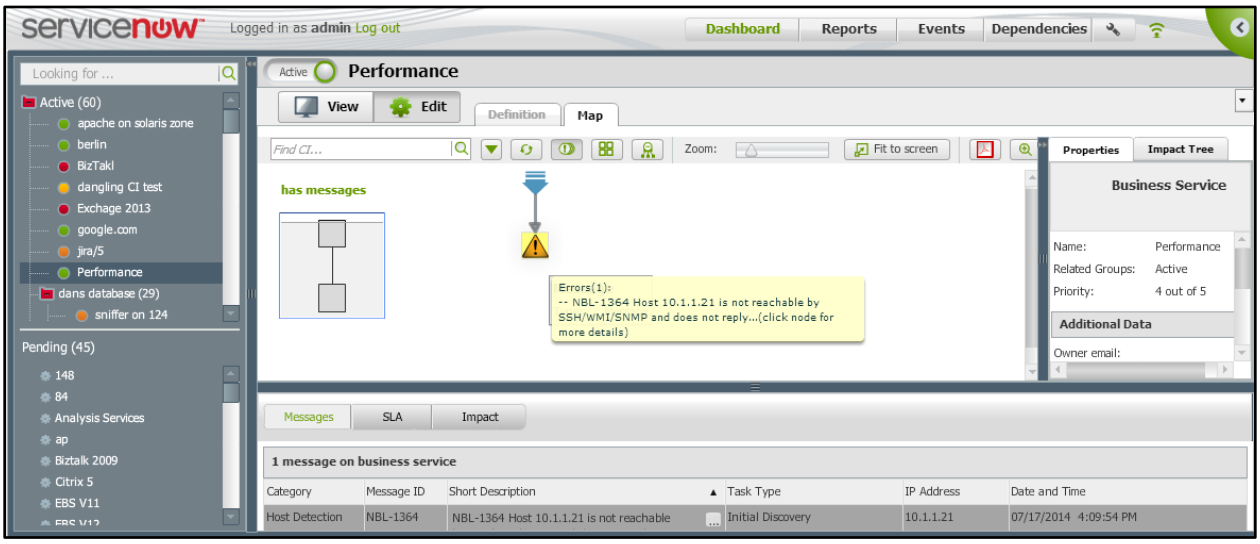
If discovery on a business service completes with messages in the **Map** panel (Figure 123), you should correct any problems. The following symbols indicate topology discovery messages. Hold the cursor over the symbol to display a tool-tip that describes the message.

-  – Message about an object.
-  – Message about a connection (arrow).
-  – ServiceWatch could not find a matching pattern and therefore does not know how to perform discovery on the object.

You may need to adjust the topology for other reasons. For example, if you determine that an object in the map belongs to a different business service, you can indicate to which business service it belongs, or you can simply exclude the object.

You can also display a network path for a connection. This does not modify the topology; it merely displays the network path in a separate dialog box.

Figure 123: Topology Map with Discovery Messages



Discovery Messages

To view all of the Discovery messages, click the **System Health** icon and select the appropriate tab:

To view the message associated with a particular message icon, hold the cursor over that icon to display a tool-tip containing a short description of its message.

A tool-tip containing the entire message is displayed when you place the cursor over the **Short Description** field of that message.

To Adjust the Business Service Topology Map

2. Retrieve and display message details. For messages that were generated by discovery, display the message as follows:
   a. Hold the cursor over the message icon to display a tool-tip containing the message.
   b. To display the messages for a particular object or connection in the bottom pane of the Dashboard, select that object or connection in the topology Map and click the **Messages** tab in the top left corner of the bottom pane.
   c. To display all the messages for a business service in the bottom pane of the Dashboard, click any blank area of the topology Map and click the **Message** tab.

Note: To adjust the height of the **Message** pane, use the cursor to grab the bar above the pane and drag it up or down.

   d. Based on the System Health message data, determine the required adjustments.
3. Perform the needed adjustments. For each object or connection that you need to adjust:

a. Right-click the object icon or connection arrow.

b. In the pop-up menu, select the adjustment type, fill in the fields of the pop-up dialog box (if any), and click OK.

Adjustment options are described in TABLE 5 for Objects and in TABLE 6 for Connection lines.

Note: Most options display a pop-up dialog box with appropriate fields.

Table 5: Topology Map Adjustment Options for Objects

Pop-up Menu Option	Description
Add connection	Displays a dialog box with fields similar to the fields in the **Entry Point** screen. Enables you to define a new entry point from the current object.
Add management host/IP	Adds an alternative IP address to a management or host IP. Useful when the currently designated IP address does not provide access.
Collapse/Collapse Outside Connections	Collapses an expanded object or group of objects
Configure NAT	Configures Network Address Translation values
Copy launch in context URL to clipboard	This URL enables another user or another application to access a specific location in ServiceWatch
Create pattern from generic CI	Displays the Create Pattern From Generic CI dialog box with fields already populated
Expand/Expand Group	Expands a compressed object or group of objects
Rediscover additional connections	Manually triggers the 'sniffing' discovery mode
Resolve credentials	Displays a dialog box that enables you to enter credential information. Useful if discovery could not continue due to lack of necessary credentials.
Resume discovery	Resumes the discovery process that had been paused
Show additional connections	Manually triggers an immediate search for additional connections.
Show CI on physical graph	Displays the Physical Topology screen for the object.
Show dependencies	Displays **Dependencies** window View panel & lists related business services
Show discovery log	Displays the log of discovery actions
Stop ignoring additional connection	Stops ignoring additional connections (if any)
Stop network based discovery from this CI Type	Prevents the discovery of other CIs or connections from all CIs of this type

Table 6: Topology Map Adjustment Options on Connection Lines

Pop-up Menu Item	Description
Add to existing business service	In the displayed dialog box, select the business service and click OK. Indicates that all objects beyond this point belong to an existing business service.
Create new Business Service from here	Create a new business service in the displayed dialog box: ✓ Fill in the business service name ✓ Select the group name (optional) ✓ Select the priority ✓ Click OK. The object below the connection arrow gets a different icon and becomes an entry point to the different business service. Connection arrows to, from, and below the object are green to indicate the flow is for a different business service.
Go to source CI	Selects the source CI which may or may not be visible on the topology Map.
Go to target CI	Selects the target CI which may or may not be visible on the topology Map.
Mark / Unmark as Boundary	Stop / allow discovery beyond this point. If an object should be excluded from discovery, use this option to mark the connector to this object as a boundary. This is useful if discovery lacks credentials to gather information about an object and you do not want to provide the credentials, or if an object should be excluded from the topology. The topology Map uses the icon to indicate a boundary you added. To remove a boundary, select **Unmark as Boundary**.
Remove Manual Connection	Removes a connection that was added manually via Add Connection. To remove a discovered connection, use **Mark as Boundary**.
Resume discovery	Enables discovery to resume from a particular node.
Show network path	Displays the network path and information about it. See Table 8 and CHAPTER 10: MONITORING NETWORKS.
Show Network Path Troubleshooting Wizard	Invokes a wizard that helps perform the network path discovery process.

Defining Object Impacts on the Business Service

This section contains the following topics

- IMPACT CONCEPTS
- DEFINING THE IMPACT OF AN OBJECT ON ITS PARENT OR BUSINESS SERVICE
- EFFECT OF TARGET DESIGNATION ON THE IMPACT TREE
- DEFINING CLUSTER IMPACTS

ServiceWatch integrates with event management and monitoring tools to indicate how events impact business services. A **Critical**, **Major**, **Minor**, **Warning**, or **Information** severity is assigned to each event. The default impact rule is that a CI affects a Business Service directly with 100% impact. CHAPTER 7: CONFIGURING EVENTS provides information about the assignment of event severity. CHAPTER 8: MONITORING BUSINESS SERVICES describes how business service severity is displayed.

Impact Concepts

ServiceWatch integrates with event management and monitoring tools to indicate how events impact business services. A **Critical**, **Major**, **Minor**, **Warning**, or **Information** severity is assigned to each event.

When an object is impacted by multiple events, it is assigned the status of the most severe of those events. For example, an object that has a Minor event and a Critical event will have a Critical status.

The status of events determines the status of the objects that they impact. However, the relationship between object status and business service status can be complex. For example, an object with a Critical status might be of negligible importance in determining the business service status, while a different, more important object with a Critical status might cause the business service status to be Critical.

The number of objects with a problematic status might also be a determining factor for the business service. For example, if only one object of a certain type has a Critical or Major status, its impact on the business service might be insignificant. However, if several objects of the same type have a Critical or Major status, the business service might become Critical.

Therefore, to determine the impact of an object's status, you must take into account a number of factors. These factors are evaluated when formulating the Impact Rules that are defined in **Impact** pane under the Topology Map.

A major aspect of an object's Impact Rule is its target, which can be either its Parent object or the Business service:

- Parent object – the object's status impacts the object directly above it in the hierarchy, which might, in turn, impact either its Parent or the Business service.
- Business service – the object's status directly impacts the Business service. Therefore, the impact on its Parent does not need to be considered.

When you define an object's Impact Rule, you are usually defining values for these factors:

- Object Status
- Resulting Target Status
- Impact Influence (the extent, shown in %, that object status affects target status)

The default impact of a cluster member on its business service is 40%.

Note: The specified **% Influence** values do *not* have to add up to 100 (see the following examples).

Example 1

A particular object has negligible importance. When you define its Impact Rule, set its **% Influence** to 0.

Example 2

A particular object is of major importance. When you define its Impact Rule, set its **% Influence** to 100.

When defining Impact Rules for clusters, you define two sets of Impact Rules:

- The impact that cluster member statuses have on the cluster status. This can be determined by the number or percentage of cluster items that have a particular status (see Example 3 below).
- The Impact that the cluster status has on its target (Business service or Parent) status.

Example 3

The Business service topology indicates a server cluster by displaying a single server icon surrounded by a cluster border. If the cluster actually contains five servers and three of them have a Critical status, the Business service status should be set to Critical. When defining the % attribute for the server, set its value to 100%.

Some objects that impact the Business service do not appear in the Topology **Map**. These include Host, Hypervisor, Network and Storage devices. ServiceWatch provides default Impact Rule values for these objects, but it is recommended that you adjust their Impact Rules according to need.

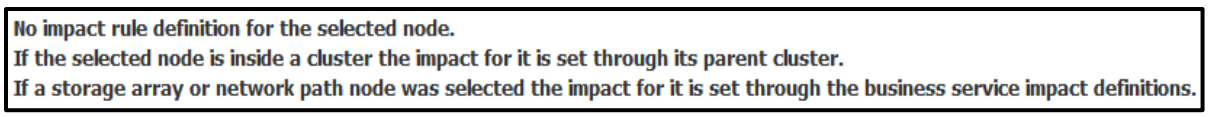
Note: Impact rules are ***not*** relevant to Technical Business Services.

Defining the Impact of an Object on its Parent or Business Service

Impact rules are defined in the **Impact** panel under the Topology **Map** in **Edit** mode.

1. To define the impact of an object, select it in the Topology **Map**. The selected object will become enclosed in a **red** box.
2. Decide if an object's status directly impacts the Business service or impacts its Parent(s) without directly impacting the Business service. Then specify appropriate Impact Rules.

Note: An object's Impact Rules can be directed toward its business service or its parent(s), but not both. If an object has Impact Rules defined toward one target (e.g., its business service) and you then define Impact Rules toward the other target (e.g., its parents), the later definition will replace the earlier definition and the earlier definition will be automatically deleted.
If you select an object for which an impact rule cannot be defined, this message is displayed:

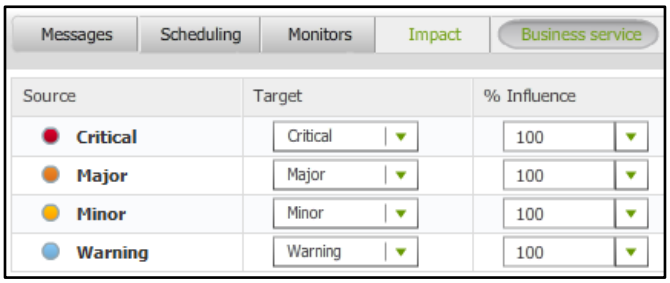


3. There are different Impact rule templates for objects with no parent, objects with one parent, objects with more than one parent, objects for which redundancy exists, and a hypervisor object. Excluding redundancy and hypervisor situations, the default rule for all of these templates is:
   the Target receives the same severity as the Source object and the % influence is 100%.

   There can be valid business reasons for changing these defaults. If a failed source object only supports a function of trivial importance to a business service, the Critical status of that object may only deserve a Warning at the Parent or Business Service level. Likewise, the 100% failure of one of the 20 children of a Parent object may deserve only a 10% Influence at the Parent level.

   a. For an object with **no parent**, the target is the **Business service** and the default template is:

Figure 124: Default impact template for an object with no parent



   If a different Target severity or % Influence is appropriate, use the down-arrows to select it.

   b. For an object with **one parent** in the Topology **Map**, the default target is the Business Service and the default template indicates the name of the parent (in this case, **iplanet**):

Figure 125: Default impact template for an object with one parent

If the status of the object does *not* directly affect its **Business service**, click the **<name of the Parent>** button so that the named parent will become the Target of the appropriate severity and % Influence values.

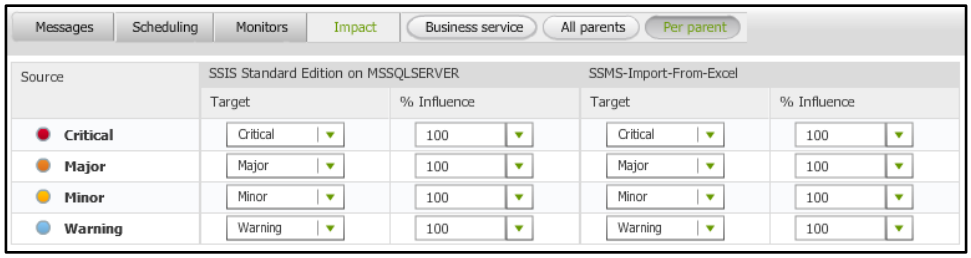
   c. For an object with **more than one parent**, the default target is the **Business service** and the default template is:

Figure 126: Default impact template for an object with more than one parent

If an object's status does *not* directly affect its **Business service**, click the **All parents** button if the *same* severity and % Influence values apply to each parent, or click the **Per parent** button if any severity and % Influence values are *not* the same for each parent.

If you click the **Per parent** button, **Target** and **% Influence** values are displayed under the name of each parent. The default template for an object with 2 parents looks like this:

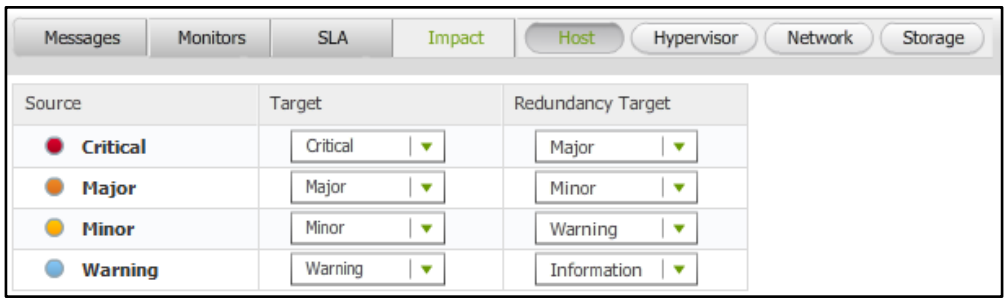
Figure 127: Default impact template for an object with 2 parents



Host

d. Redundancy is presumed to exist if the **source** is a **Host**, the **Network** or a **Storage** device. The Target is the parent of the Source and Redundancy Targets are components that can perform the function of the parent. Because a Business service can have any or all of these source-types, you can select any or all of them, one after the other, and specify the appropriate Target and Redundancy Target severities. By default, the **Target** severity is identical to the **Source** severity and the **Redundancy Target** severity is one level lower than the **Source** severity. **% Influence** is not relevant for a Host, Network or Storage device.

Figure 128: Host impact template



Hypervisor

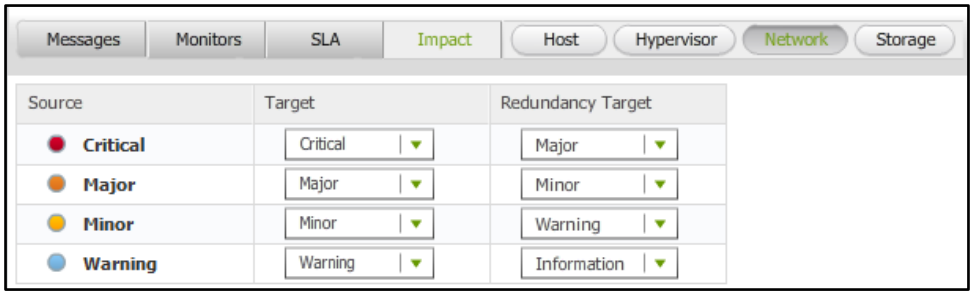
e. Redundancy does *not* exist if the source is a **Hypervisor** and % Influence is not relevant. The **Target** is the parent of the Hypervisor and by default the Target severity is identical to the Source severity.

Figure 129: Hypervisor impact template

Network

f. If the source is the **Network**, the **Target** is the Business service and the **Redundancy Target** is an alternate path on the same network.

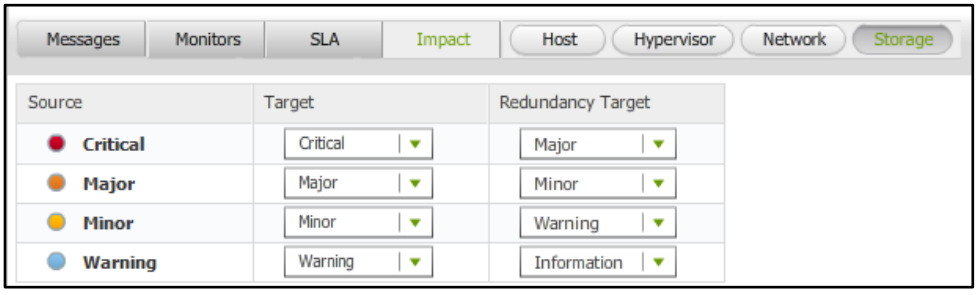
Figure 130: Network impact template



Storage

g. If the source is a **Storage** device, the **Target** is the Business service and the **Redundancy Target** is an alternate Storage device. .

Figure 131: Storage device impact template



Effect of Target designation on the Impact Tree

a. If you change the impact Target from **Business service** to **<name of parent>**, **All Parents** or **Per Parent**, the **Impact Tree** reflects the change immediately. Figure 132

shows the Impact Tree for an object whose impact Target is the Business Service. Figure 133 shows the Impact Tree for the same object when its impact Target is All Parents or Per Parent.

Figure 132: Business Service Impact Tree of a 2-parent object

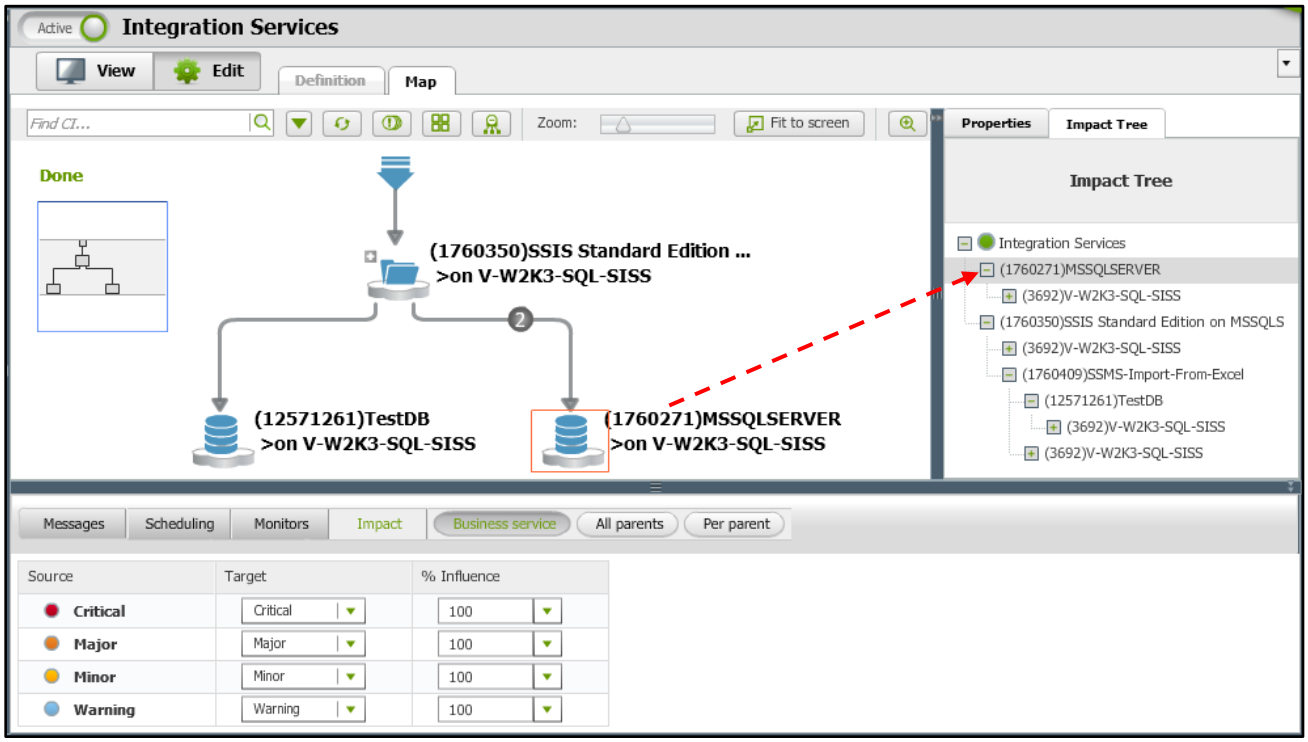
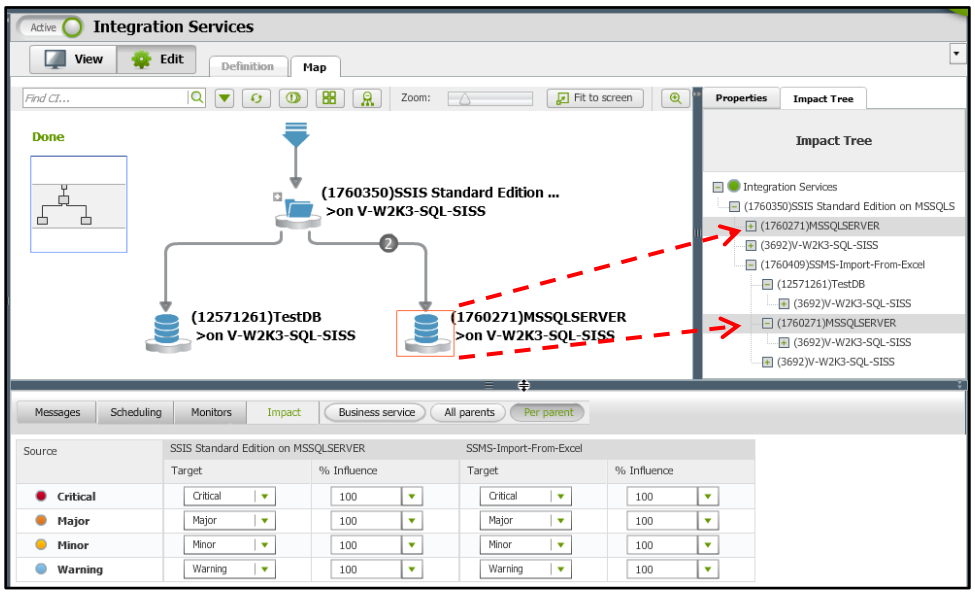


Figure 133: Per Parent Impact Tree for the same 2-parent object



Defining Cluster Impacts

When defining the impact of a cluster on a business service, you define two sets of Impact Rules:

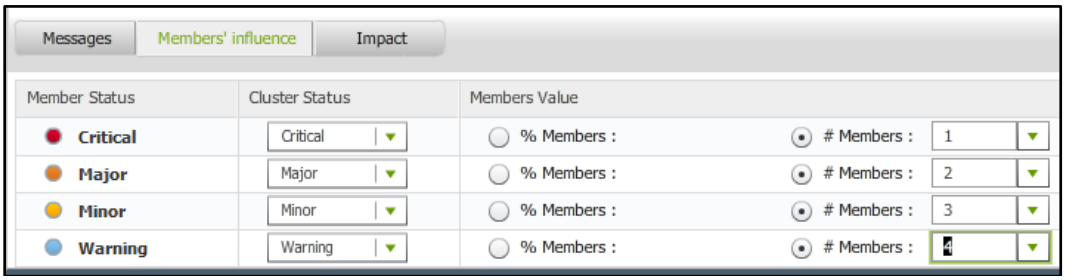
- To show the impact that cluster members have on cluster status, click **Members' influence**, click the **% Members** or **# Members** radio buttons, and use down-arrows to set the desired values.

  Objects in the cluster are not displayed. Therefore, you cannot define the impact of specific members. Instead, you define *either* the number of cluster objects *or* the percentage of the objects in the cluster that will be used to determine the cluster status.

  Examples

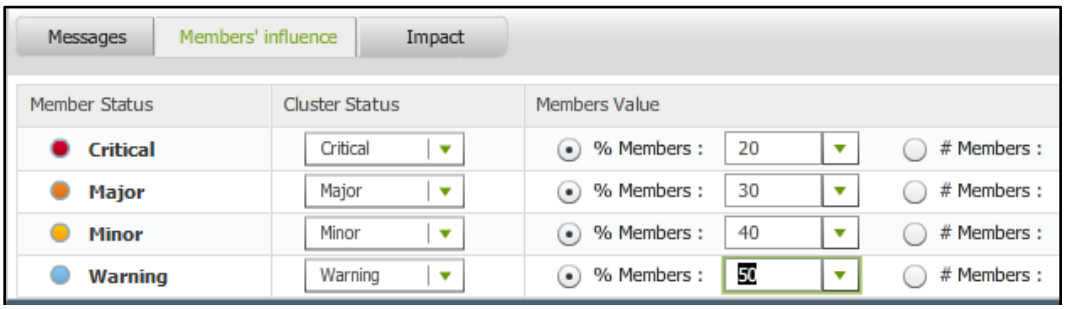
  ✓ If 1 cluster member has the status of **Critical**, the cluster status is set to **Critical**.
  If 2 cluster members have the status of **Major**, the cluster status is set to **Major**.
  If 3 cluster members have the status of **Minor**, the cluster status is set to **Minor**.
  If 4 cluster members have the status of **Warning**, cluster status is set to **Warning**.

Figure 134: Cluster impact – Number of Members template



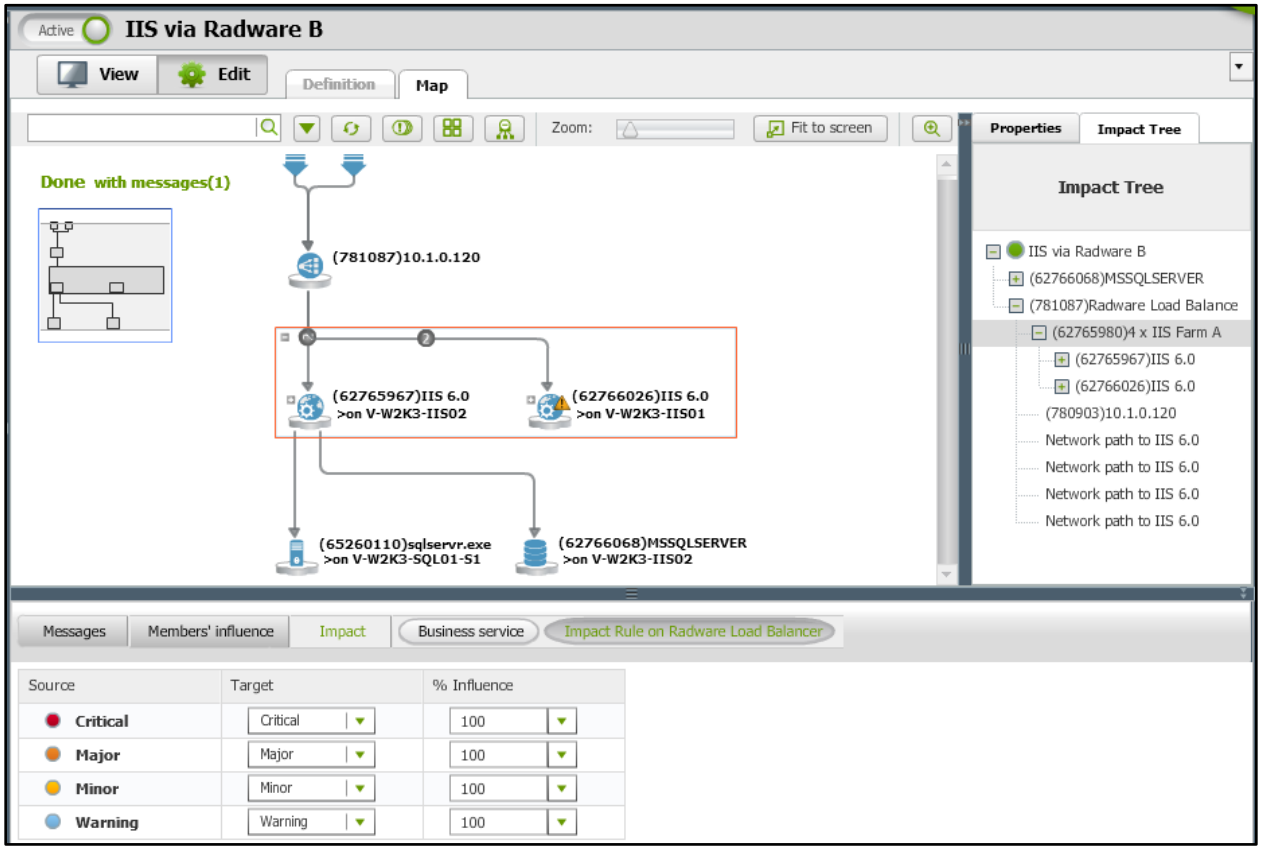
  ✓ If 20% of the members have a status of **Critical**, cluster status will be set to **Critical**.
  If 30% of the members have a status of Major, the cluster status will be set to **Major**.
  If 40% of the members have a status of Minor, the cluster status will be set to **Minor**.
  If 50% of the members have a status of Warning, cluster status will be set to Warning.

Figure 135: Cluster impact – Percentage of Members template



- To show the impact that a cluster has on its target, click Impact, click Business service or <name of parent>, then use the down-arrows to set the Target severity and % Influence values. For instructions, see Defining the Impact of an Object on its Parent or Business Service on page 143.

Figure 136: Defining Cluster Impact on its Target (Business service or <name of parent>)



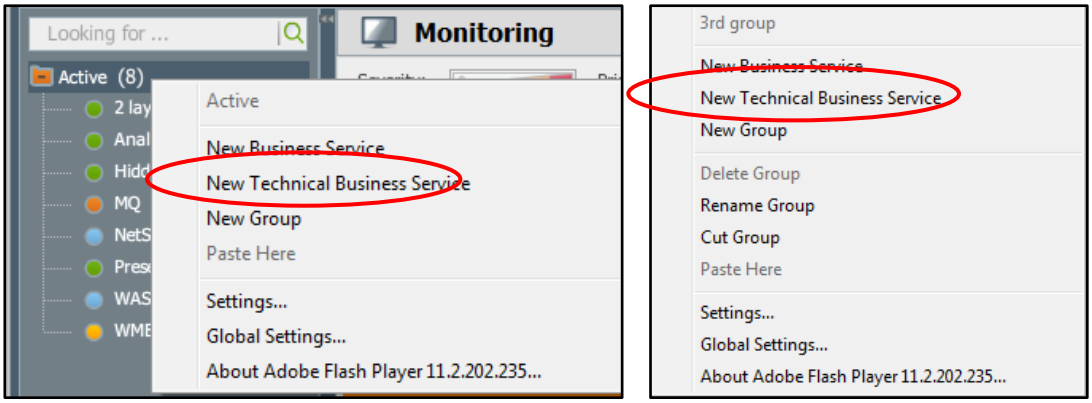
4. When you finish defining Cluster Member and Cluster impacts, exit **Edit** mode. The changes you made are automatically saved

Creating Technical Business Services

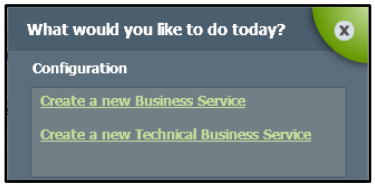
Technical business services are manual collections of objects. For example, to track the status of all Apache servers, you can define a technical business service called 'Apache' and define a query that selects all Apache servers for that technical business service. The wizard that defines technical business services is *not* the same wizard that defines regular business services.

1. To create a technical business service, right-click the Active root, or any node above the CI level in the Active tree, and select New Technical Business Service in the pop-up menu

Figure 137: New Technical Business Service option in pop-up menus

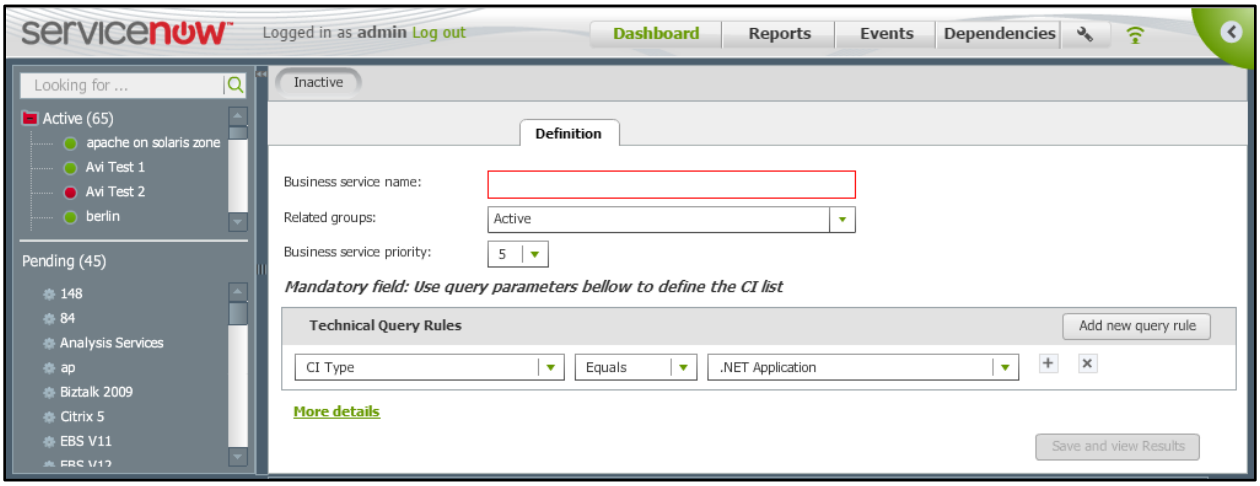


or click the green quadrant in the top right corner  and select the Create a new Technical Business Service link in the **What would you like to do today?** pop-up.



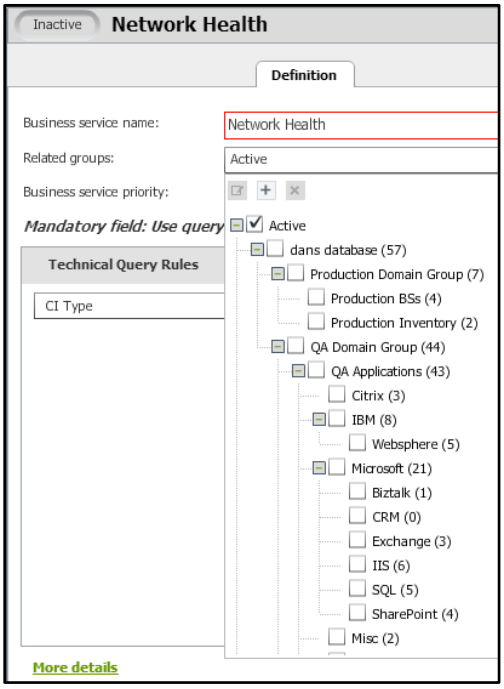
2. The Definition panel of the Technical Business Service wizard (**FIGURE 138**) is displayed.

Figure 138: Technical Business Service – Definition panel with Technical Query Rules pane



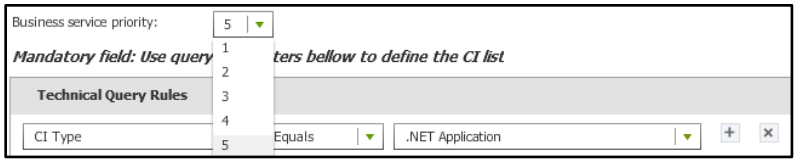
3. Type in the Technical **Business service name**. As you type each letter, it is also displayed in the header of this screen.
4. If this technical business service should belong to a group, click the **Related groups** down-arrow and select the checkbox of that group. In this example, the **Active** node has been selected.

Figure 139: Related groups field in Definition panel



5. Click the Rename group  , Add group  , or Delete group  icon to perform its function.
6. Select a value (low=1; high=5) from the **Business service priority** drop-down list (Figure 140).

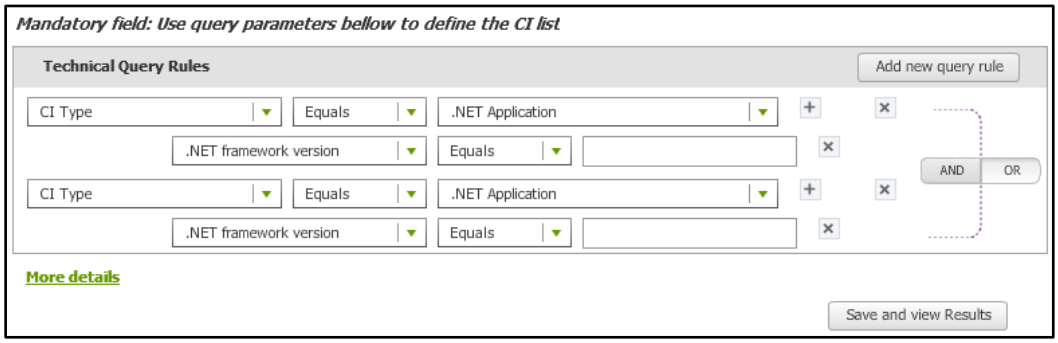
Figure 140: Technical Business Service priority drop-down list



7. Click 

at the right corner of the **Technical Query Rules** header to display an area for adding a query rule.

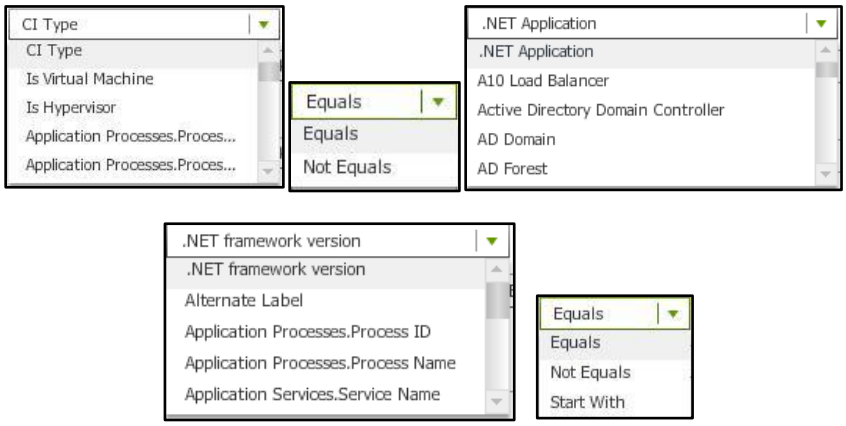
Figure 141: Technical Business Service – Technical Query Rules



Specify the query that selects the components or elements that constitute this Technical Business Service. For each component/element to be included:

a. Click the down-arrow for each field to display a list of valid values for that field.

Figure 142: Technical Query Rules drop-down lists



b. Select the subject of the query (for example, CI Type or Is Virtual Machine). The relational operators and values for the query vary according the selected subject.
Next, do the following:
   i. If a relational operator drop-down list is displayed, select the relational operator.
   ii. Select (or fill in) the value that is to be matched.
   iii. If  is displayed ***next*** to a query line, click it to add an additional value to be matched.

c. If  is displayed in the header, you can click it to add an additional query subject and display the AND / OR relational operator buttons. By default, **AND** is selected and grayed-out; **OR** is not grayed-out and can be selected  .

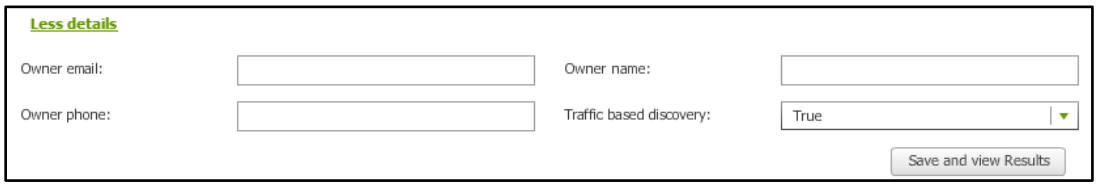
d. To change this relational operator to OR, ***single***-click either button. **OR** becomes greyed-out indicating it is selected; **AND** becomes not grayed-out so it can be selected  .

Note: The AND / OR buttons toggle. Double-clicking either button will toggle this operator twice, resulting in no change.

e. To remove any query detail, click the  icon on its line. .

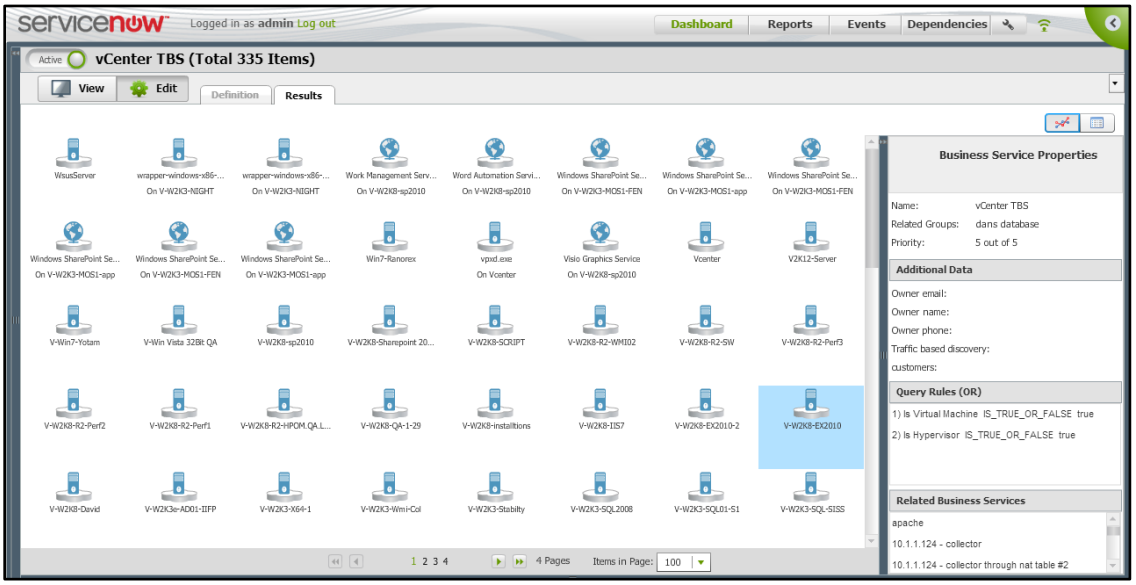
8. To specify an optional Owner name, phone, email address, Customers who use this business service, and/or to specify whether Traffic based discovery is (true) or is not (false) used, click the **More details** link. To hide these fields, click the **Less details** link.

Figure 143: Technical Business Service – More details fields



9. When you finish defining the query details, click  to generate and display the results in the **Results** panel (Figure 144). The default state of each new technical business service is Inactive and it is listed in the **Pending** panel on the Dashboard.

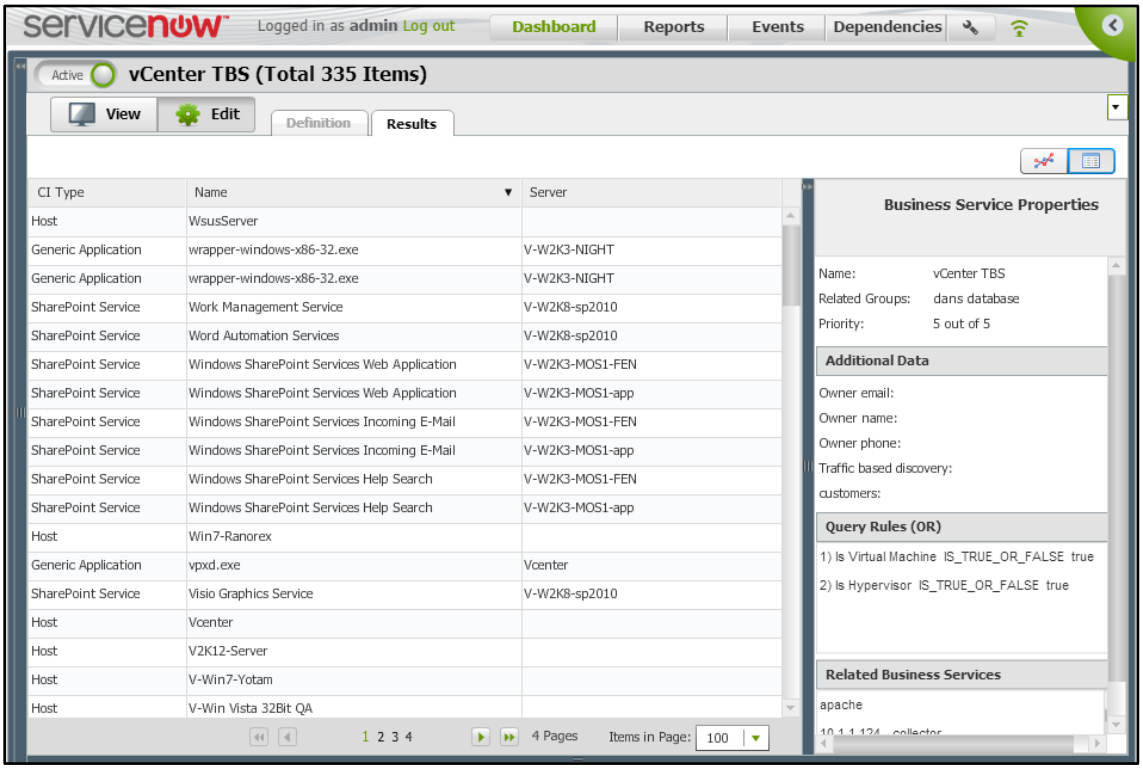
Figure 144: Technical Business Service Results



10. While in the **Results** panel, you can:

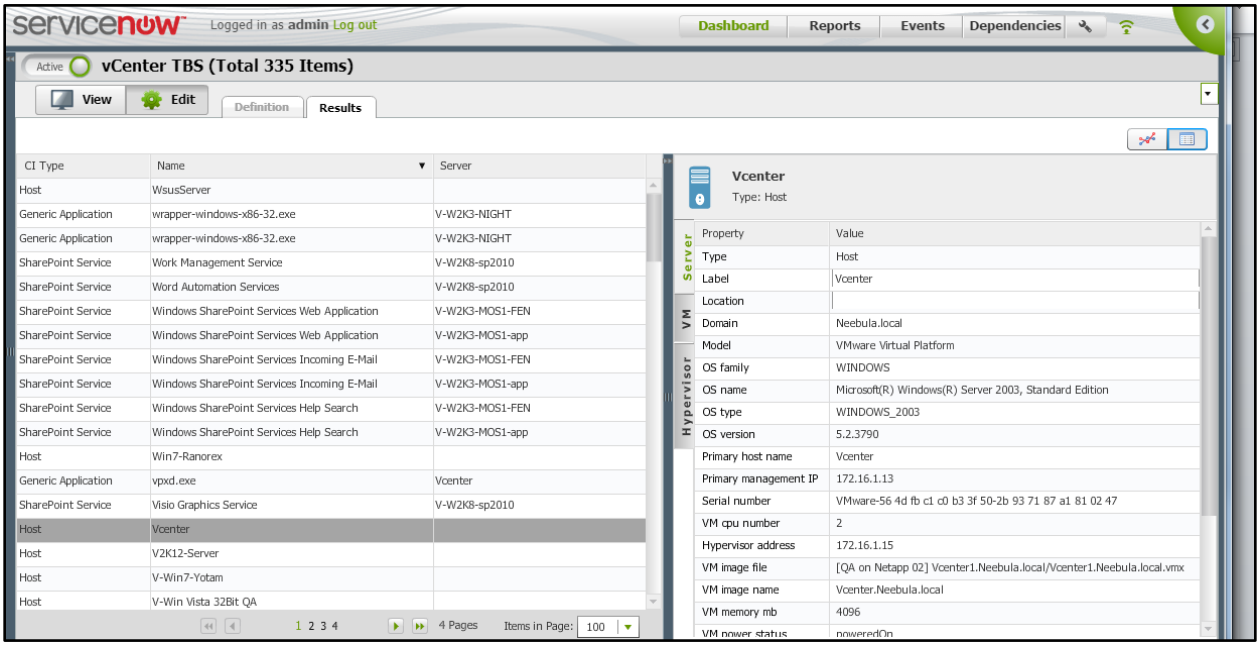
- Click the  graph display button or  table display button to display each element as an icon (as in Figure 144) or as a row in a table.

Figure 145: Technical Business Service – Results panel table display



- Display the Element Properties of an object by clicking the object in either graph or table mode.

Figure 146: Technical Business Service – Element Properties



11. To activate this technical business service, click 

.

The business service's state indicator will change to 

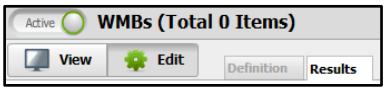
and it will move from the **Pending** panel to the **Active** tree.

12. To disable this technical business service, click 

. The business service's state indicator will change to 

and it will move from the **Active** tree to the **Pending** panel.

13. When the business service is 

, the **View/Edit** 

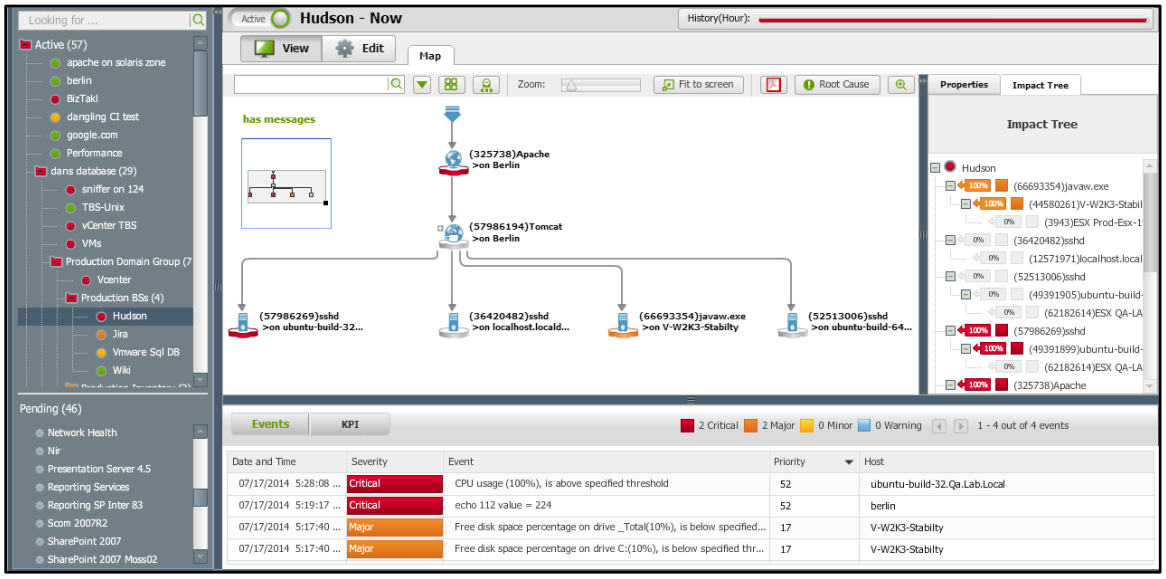
toggle buttons are displayed. Click **View** to view the **Results**. Click **Edit** to edit the **Definition** or **Results**.

Root Cause Analysis

When a CI topology **Map** is displayed in **View** mode, click 

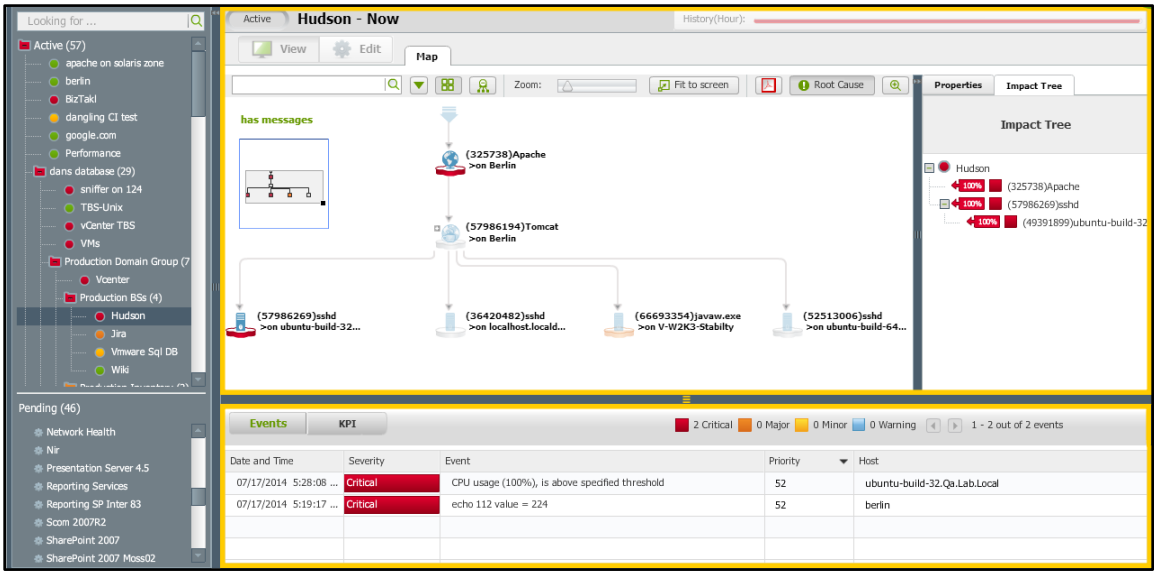
to toggle into and out of **Root Cause** mode. When *not* in **Root Cause** mode, topology nodes are not grayed-out and all of the Element Properties, Events and KPIs can be displayed (Figure 147).

Figure 147: Topology Map and Impact Tree when *not* in Root Cause mode



When *in* **Root Cause** mode, topology nodes that are *not* responsible for the business service status *are* grayed-out, the **View** and **Edit** buttons are grayed-out, and only **Element Properties**, and **Events** or **KPI**s that are responsible for the current business service status are displayed. In addition, the borders surrounding the top and bottom panes of the business service screen become **yellow** (Figure 148).

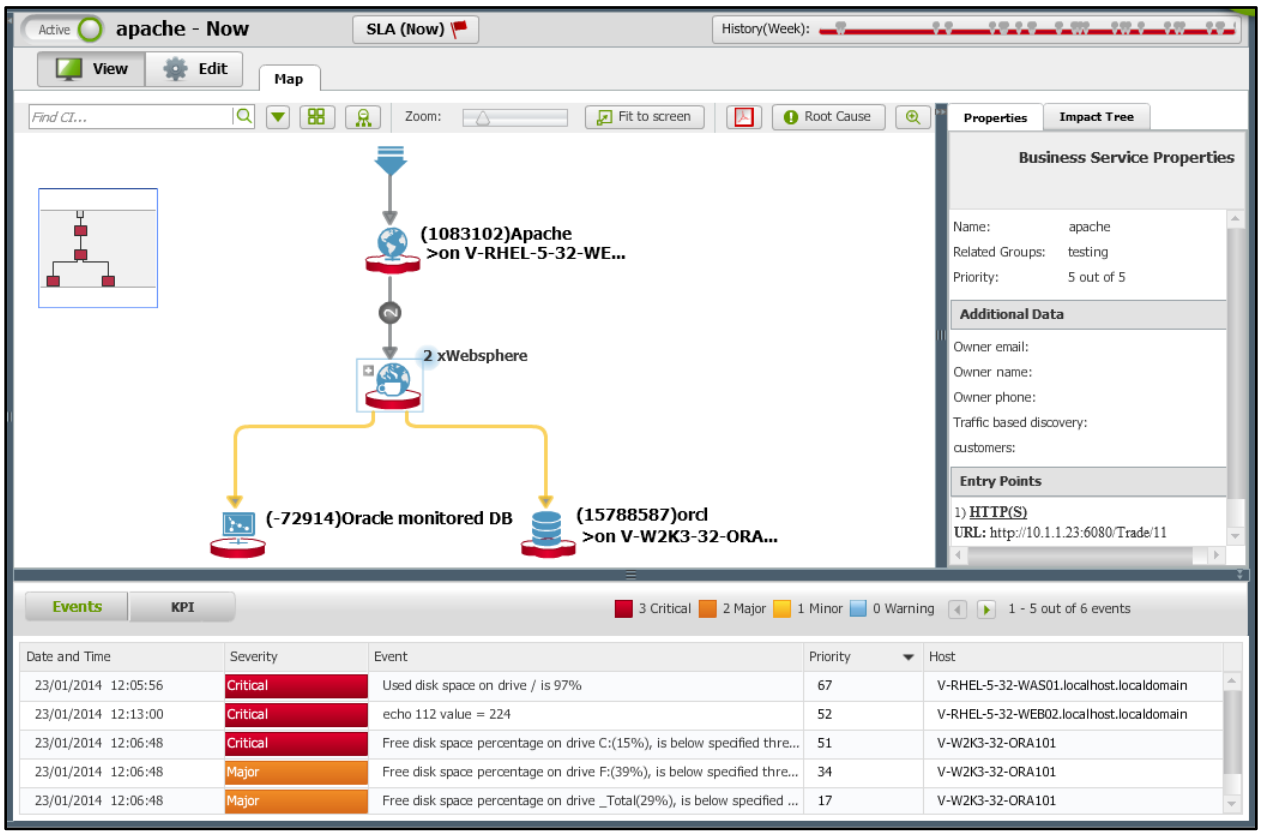
Figure 148: Topology Map and Impact Tree in Root Cause mode



Business Service, Object or Connection Properties

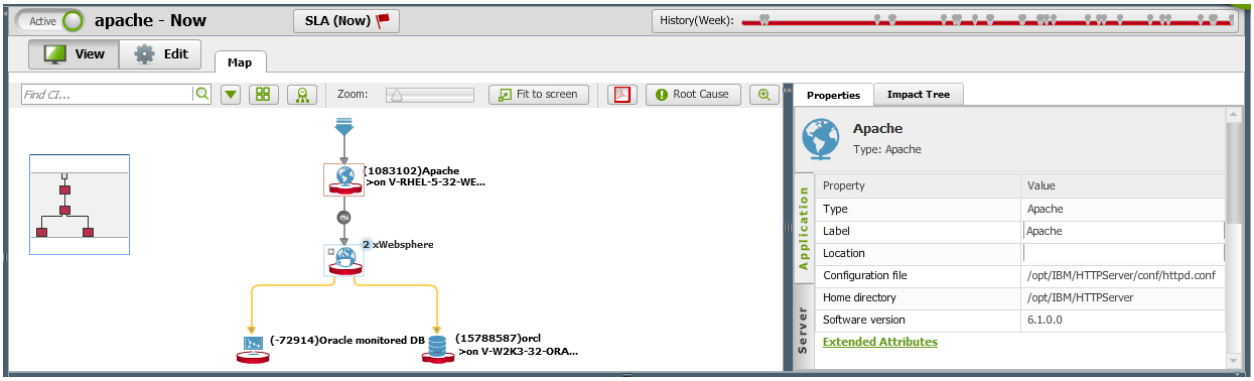
To view the properties of an active or inactive business service, click its topology **Map** background and then click the **Properties** tab in the top right pane. Its **Business Service Properties** are displayed.

Figure 149: Business Service Properties panel



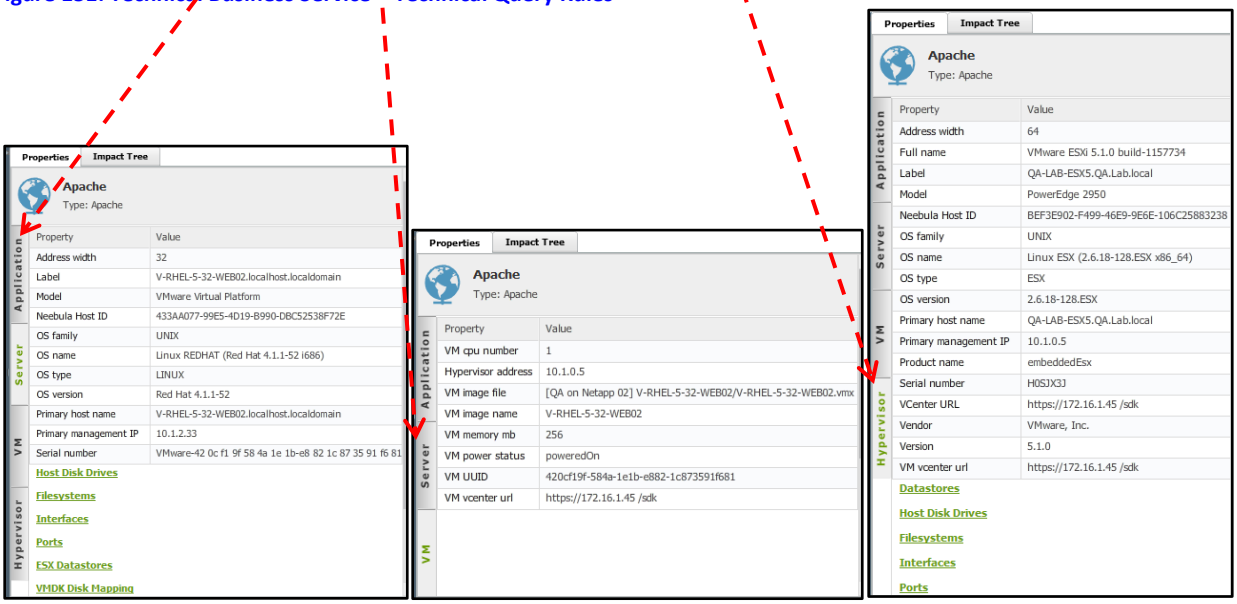
To view the properties of a CI object, click it in the **Map** panel and click the **Properties** tab in the top right pane. The object's **Application** properties are displayed (Figure 150).

Figure 150: Element Properties panel



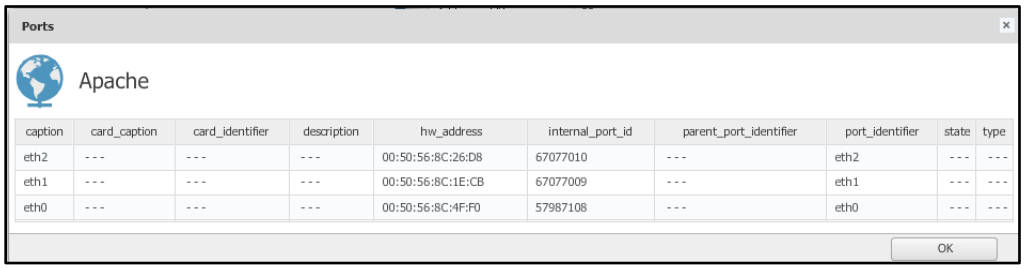
To display *simple* **Server**, **VM** (virtual machine) or **Hypervisor** properties (if any), click the appropriate vertical tab. Properties that have a single associated value are displayed in a list.

Figure 151: Technical Business Service – Technical Query Rules



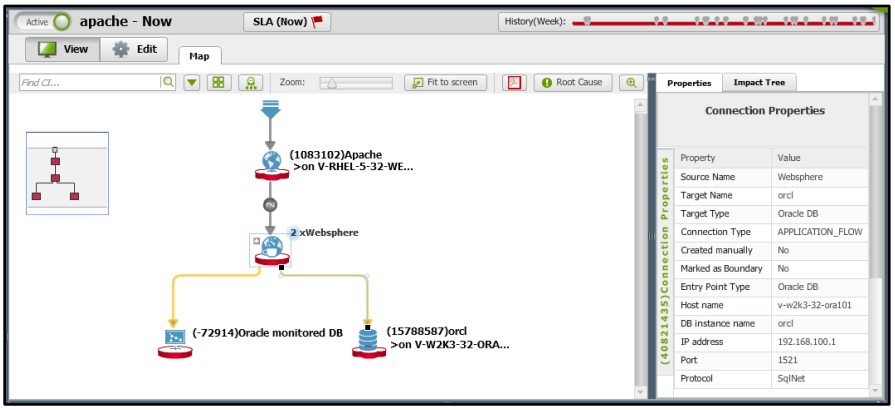
To display *complex* **Application**, **Server** or **Hypervisor** properties, click their **blue** or **green** underlined links. E.g., clicking **Ports** in the **Server** properties panel will display a **Ports** table.

Figure 152: Technical Business Service – Ports table



To view connection properties, click the connection in the **Map** panel. Two small black squares indicate its end points. Click the **Properties** tab in the top right pane to display the **Connection Properties** panel.

Figure 153: Connection Properties panel



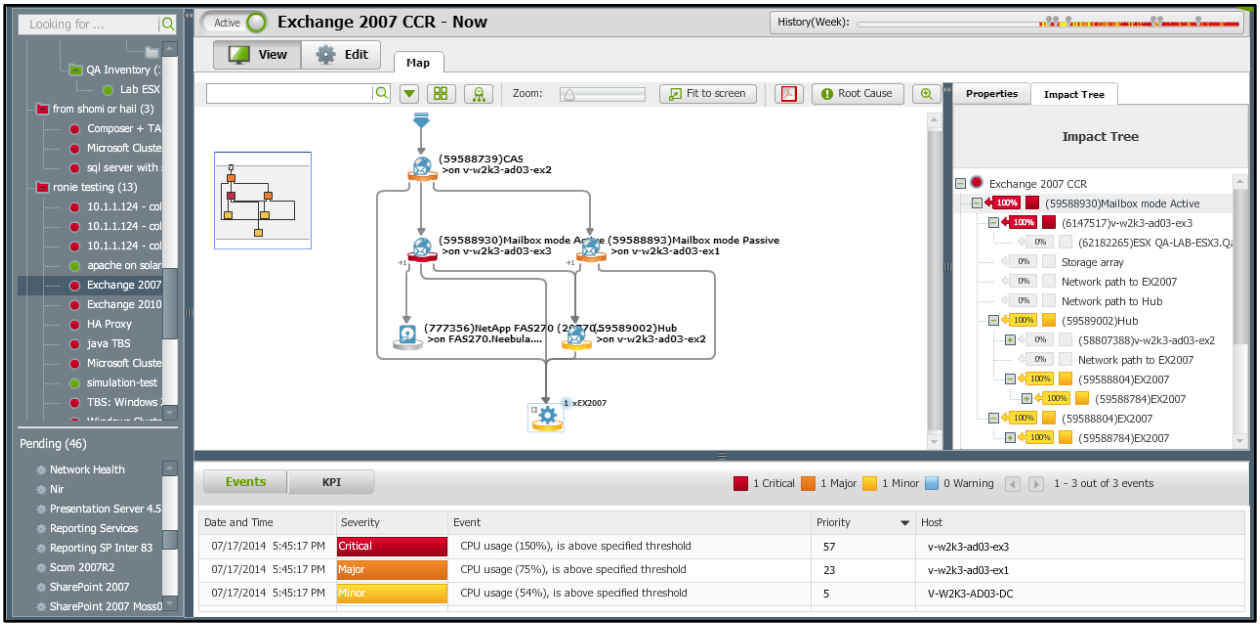
Viewing the Impact Tree of a Business Service

As described in DEFINING THE IMPACT OF AN OBJECT ON ITS PARENT OR BUSINESS SERVICE on page 143, you can define a component's impact in the **Impact** panel underneath the topology **Map** in **Edit** mode.

You can view the health of a component by displaying its business service **Impact Tree** panel on the right of the topology **Map** in **View** mode. Click the business service you want to view in the **Active** tree, or double click the tile or bubble of that business service in the Dashboard. If the topology **Map** is not displayed in **View** mode, click 

. Click the **Impact Tree** tab in the top right panel.

Figure 154: Impact Tree panel of a topology Map in View mode



In the **Impact Tree** panel, the color of the circle indicates the Severity level of the Business Service. The color of each square indicates the Severity level of that component. The color of each 

symbol indicates the Severity level and percentage effect of that component on its parent.

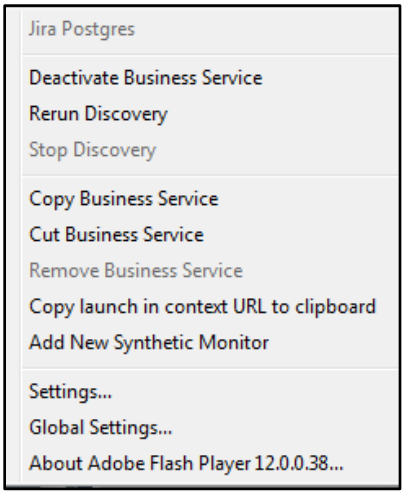
Working with Existing Business Services & Groups

You can perform certain actions on business services and groups. For example, you can move or copy existing business services to an existing group, or remove a business service from a group.

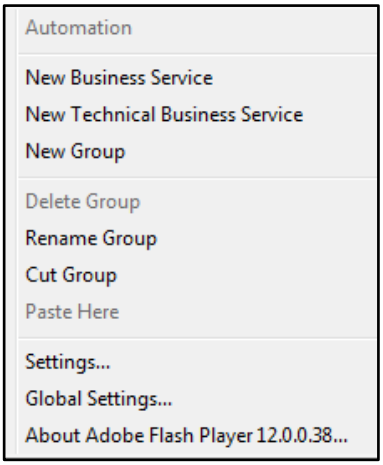
You generally do this by right-clicking the appropriate entity and selecting the appropriate action from the pop-up menu. TABLE 7 explains how to perform the most common actions.

Figure 155: Right-Click Menus for Groups and for Active and Pending Business Services

Active Business Service



Business Group



Pending Business Service

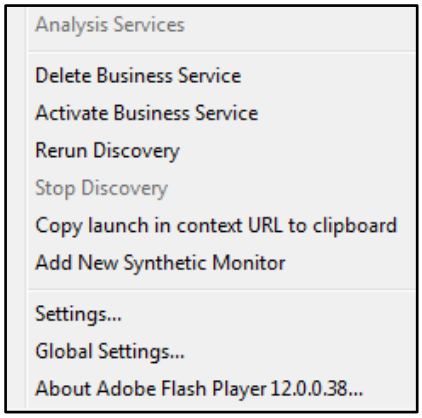


Table 7: Group/Business Service Manipulation

Action	Do the following in the Active or Pending tree
Activate a business service	Right-click the business service in the **Pending** tree. Select **Activate Business Service** *or* select the business service and toggle the **Inactive** icon to **Active**. The business service moves from **Pending** to **Active**.
Deactivate a business service	Right-click the business service in the **Active** tree. Select **Deactivate Business Service** *or* select the business service and toggle the **Active** icon to **Inactive**. The business service moves from **Active** to **Pending**.
Move (or copy) a business service to a group	Right-click the business service and select **Cut** (or **Copy**) **Business Service**. Right-click the group and select **Paste Here**.
Remove a business service from a group	Right-click the business service in the group and select **Remove Business Service**.
Delete a business group	Right click the group and click **Delete Group**. **Caution:** All business services in the group are deleted with the group.
Rename a business group	Right click the group and click **Rename Group**. Then enter the new **Group name** in the **Rename Group** dialog box.
Rename a business service	If the business service is **Active**, deactivate it as described above. When it is **Pending**, click the **Definition** tab, change its name in the **Business service name** text box, and optionally activate it as described above.
Display/hide a group's business services	Expand or collapse the business group node in the **Active** tree.

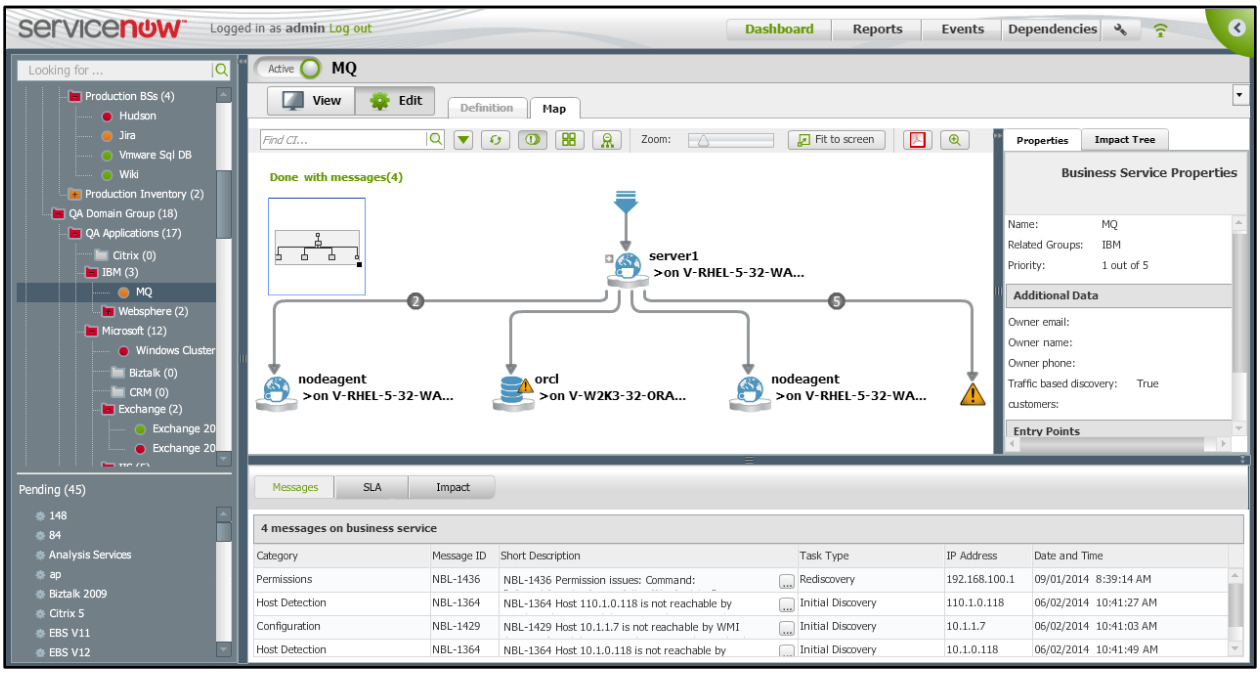
Editing a Business Service

Displaying a business service in Edit mode lets you:

- modify entry points (See Entry Point Types)
- modify its topology by adding manual connections
- change its business service structure (mark as a boundary or create a new business service)
- fix discovery messages by adding missing credentials or configuring management access
- manage how components affect the business service by changing impact definitions
- specify which monitors are active for which CIs
- specify SLA rules, details, Events and KPIs.

Topology Map

Figure 156: Topology Map panel in Edit mode



To edit a business service click its node in the **Pending** tree, or click 

after you

- click the business service's node in the **Active** tree, or
- double-click its tile in the **Tile** Dashboard, or
- place the cursor over its bubble in the **Bubble** Dashboard and click **See topology** in its tooltip

To return to the top level of the Dashboard, click 

or the **Active tree** root.

Adjusting the Topology Map

While working in the **Map** panel, you can make various adjustments to the screen display.

Figure 157: Map manipulation icons in View mode

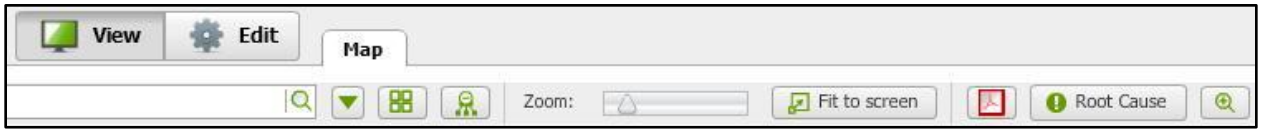
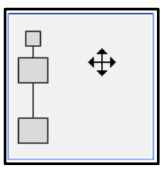
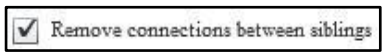


Figure 158: Map manipulation icons in Edit mode

TABLE 8 lists topology map manipulation actions. Some actions are not available in some maps.

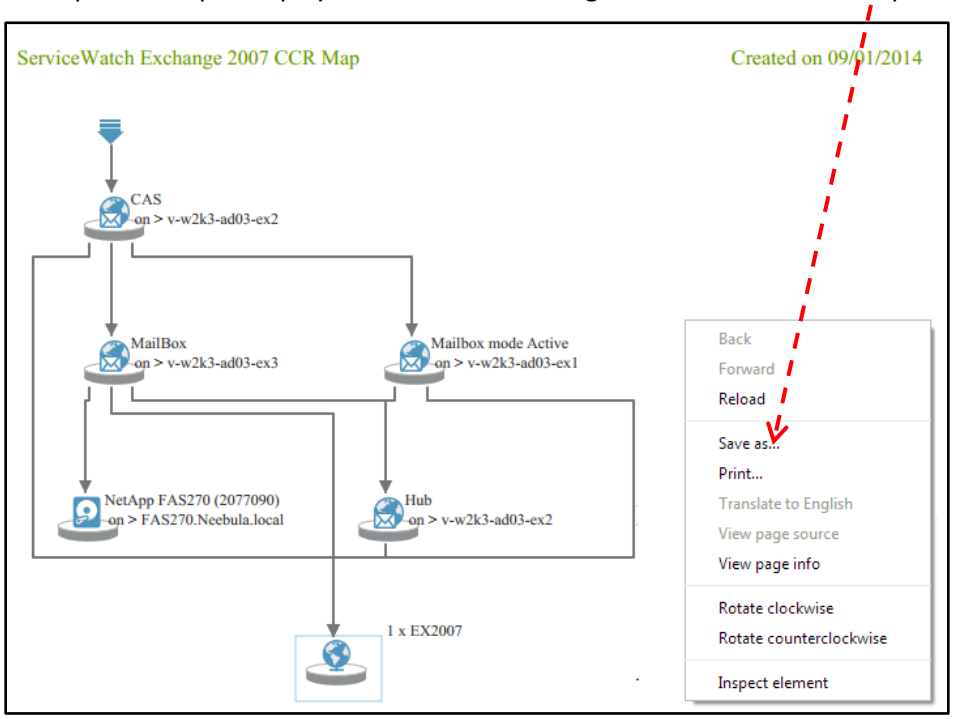
Table 8: Topology Map manipulation actions

Desired Action	Relevant Icon	How to do it
To group undiscovered CIs and messages by source CI		In **Edit** mode, click this icon. To re-display the original Map, click this icon again.
To gray-out all CI icons except the root cause CI		In **View** mode, click the **Root Cause** button. Click it again to view the usual display.
To refresh the topology Map display		In **Edit** mode, click the **Refresh** button.
To list only CIs that contain the specified text string in the **Active** *and* **Pending** panels		Type the string in the Search text box.  is *not* clickable.
To display the Network Path for a connection between components	(no icon)	Right click the connection and select **Show network path** in the pop-up menu. **Network Path** & **Map** functionality are similar. See CHAPTER 10: MONITORING NETWORKS.
To adjust the size of the icons in the display		Move the **Zoom** slide at the top of the screen.
To set the display size to fit the screen		Click the **Fit to screen** button
To shift the displayed area of a skeleton when all of the skeleton does not fit inside the panel		Move the cursor into the thumbnail at the top left of the panel. Hold down the left mouse button and move the 4-arrow cursor inside the thumbnail.

Desired Action	Relevant Icon	How to do it
To hide/display the overview thumbnail		Click the **Overview** icon at the top center of the Map.
To display hosts (and host connections) instead of the applications running on them.		Click the icon. It will become grayed-out. Click it again to redisplay the applications.
To display/hide a magnifier for enlarging an area of the Map		Click the **Magnifier** icon at the top right corner of the Map. Move the cursor over the area to magnify. Click the icon again to toggle off magnification.
To display additional options		Click the icon.
Hide/display sibling connections		Click  and select/clear the checkbox. Connections are only hidden and *not* disconnected.
Export a map		In **View** mode, click the icon. The pdf file is displayed. You can Print it or Save as … .

Exporting a Topology Map

To export the currently displayed topology Map as a PDF file, click the **Export Map** button  in the **Map** panel. The exported map is displayed. You can use the right-click menu to save or print it.



Chapter 7: Configuring Events

This chapter contains the following topics:

Displaying Events

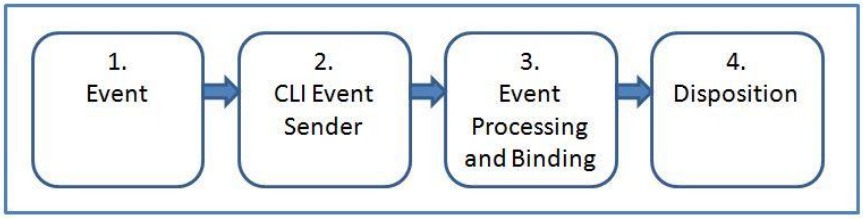
Event Management Systems (EMSs) monitor computer networks and detect significant events. These events may trigger alerts (e.g., SMSs) and be displayed by the EMS application.

ServiceWatch integrates with your existing EMS and uses event information provided by the EMS to determine how the event affects configuration items in your system and how it impacts your business services. This enables you to take appropriate steps to keep your business services running and healthy.

Event Processing Flow

Figure 159 shows the steps in the Event Processing flow, from event detection by an EMS through event handling by ServiceWatch. A description of these steps is provided after the figure.

Figure 159: Event Processing Flow



1. The EMS detects an event based on thresholds and triggers an alert.
2. The Command Line Interface (CLI) Event Sender is triggered by the alert and sends an event to the ServiceWatch server.
3. Event Processing and Binding – ServiceWatch uses parameters extracted from the event and user-defined processing rules to determine which business service is impacted by the event and the severity of the impact. Where possible, ServiceWatch determines the configuration items (CIs) impacted by the event and binds the event to the CIs.
4. Disposition – ServiceWatch performs these actions:
   - ✓ It displays the relevant information in the Monitor facility interface.
   - ✓ It sets business service severity to the severity of the most severe event that impacts the service.
   - ✓ It stores the information if the event is bound to a CI. Otherwise, it eventually discards the data. By default, a maximum of 2000 unbound events are retained in the system while it is running.
   - ✓ It displays stored events that have a severity range of **Warning** – **Critical**. Unbound events that have not yet been discarded can also be displayed. It does not display other events.

Information Transfer of EMS Events to ServiceWatch

EMS event details are generally provided in the format: *EMS_field=value*.

The following types of information are most important to ServiceWatch:

- Data that helps identify objects (Configuration Items). For example, *field_x= PostgreSQL* ***SID down*** indicates that an instance of PostgreSQL is down. ServiceWatch uses this data to bind the event to the configuration item, after which it identifies the business service in the topology where the configuration item occurs.
- Data that helps identify event characteristics such as severity, priority, and resolution status (e.g., *field_y*=**Critical**). ServiceWatch uses this data to monitor the system and provide up-to-date information about your business services.

ServiceWatch enables you to specify which event fields should be sent to the ServiceWatch server.

As indicated in EVENT PROCESSING FLOW, the CLI (Command Line Interface) Event Sender is triggered by an alert and is responsible for sending information to the ServiceWatch server. The CLI Event Sender is a ServiceNow-supplied utility called **nblevent**. This utility receives event parameters from the alert and places selected parameters into a command line that it sends as an http request to the ServiceWatch Server.

For this mechanism to work, you must define the command line to the `nblevent` utility, making sure to specify which event fields should be included in the http request. For instructions, see DEFINING THE EVENT COMMAND LINE.

ServiceWatch Predefined Event Fields

Although every EMS provides similar event data, each EMS has its own naming conventions. To handle event data from various EMSs, ServiceWatch has predefined alert fields that can be mapped to corresponding EMS fields (see Table 9). However, in addition to these predefined ServiceWatch fields, you can send any EMS-generated field to ServiceWatch.

Notes:

- Fields with a single asterisk in the Note column are mandatory and must be sent to ServiceWatch with the name shown in the Predefined Field column.
- Fields with a double asterisk in the Note column are mandatory and must either come to ServiceWatch with the name shown in the Predefined Field column, or be extracted from the text field by Binding rules, or be mapped using Event Source rules.

Table 9: Predefined Event Fields

Note	Predefined Field	Description
	businessServiceName	Business service name
	ciTypeName	CI type name
*	**emsSystem**	EMS system that sent the event
	expireTime	Time at which the event is no longer relevant
	hostAddress	Host name or IP of the CI to which event should be bound
**	**messageKey**	Unique identifier for a message. When a new event with the same messageKey arrives, the old active event is closed.
	ownerID	Owner name or ID
	resolutionState	Event resolution state. Values: NEW,CLOSED
**	**severity**	Event severity: INFORMATION, WARNING, MINOR, MAJOR, CRITICAL
	state	Event state. Values: UNKNOWN, NOT_OWNED, OWNED, ACKNOWLEDGED, DELETED
	text	Text of the event, used by Binding rules to help determine the CI. For example, ORAxxx indicates an Oracle-related event

Integrating ServiceWatch with Your EMS

To integrate ServiceWatch with your EMS, perform these steps:

1. Define the Event Command Line

   The Event Command Line identifies the event fields that the **nblevent** utility should send to the ServiceWatch server. For instructions, see DEFINING THE EVENT COMMAND LINE on page 170.

2. Define Event Source rules

   An Event Source rule matches EMS event fields with their corresponding ServiceWatch fields (see SERVICEWATCH PREDEFINED EVENT FIELDS) and, for each pair of fields, translates EMS values to their corresponding ServiceWatch values. For instructions, see MAPPING EMS FIELDS TO SERVICEWATCH FIELDS on page 170.

3. Define Binding rules.

   A Binding rule selects (extracts) information from unbound events sent by the command line interface (CLI) and, depending on the information, maps it to object attributes or to new or existing event fields.

   ✓ Extracted information that can be mapped to object attributes helps determine the configuration item type to which the event relates, which in turn helps ServiceWatch bind the event to the configuration item (CI).

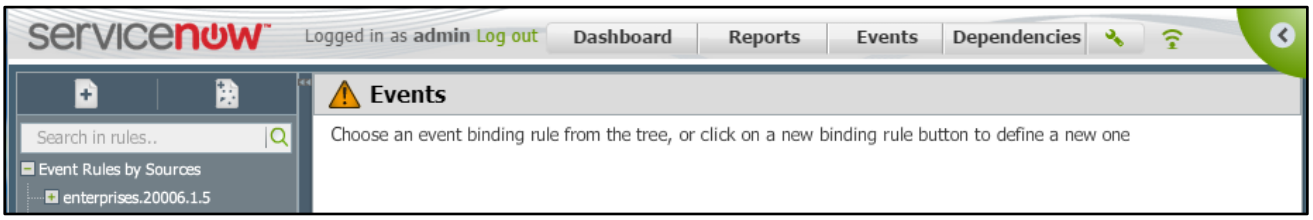
   ✓ Other extracted data mapped to event fields can provide ServiceWatch with useful information (for example, for determining the severity of the event).

   For instructions about defining Binding rules, see EXTRACTING AND BINDING EVENT INFORMATION on page 173.

Event Source rules and **EMS Mapping** rules are defined in the **Event Source Definition** window (Figure 164).

If you are *not* already in an **Event Source** or **Binding Rule Definition** window, click the **Event Sources/Rules** link in the **Settings** menu to display an empty **Events** window.

Figure 160: Empty Events window



From anywhere in the hierarchy of **Event Sources/Rules** windows, click the  icon to display an empty **Event Source Definition** window.

Event Rules by Sources tree

The **Event Rules by Sources** tree contains three nested levels:

1. Event Source (Event Management System)
2. Configuration Item type

3. Binding Event rule (defined for the CI under the Event Source)

   The **New Binding Rule** icon and the **New Event Source** icons are at the top of the **Event Rules by Sources** tree.

   To define a new Event Source rule, click and perform the steps described in Mapping EMS Fields to ServiceWatch Fields on page 170.

   To define a new binding rule for unbound events, click and perform the steps described in Extracting and Binding Event Information on page 173.

   To edit an existing rule, select that rule in the **Event Rules by Sources** tree. You can filter the nodes displayed in this tree by typing a character string in the Search in rules.. text box. Nodes containing a rule that contains that character string will be displayed.

Unbound Events Table modes

To display the **Unbound Events Table**, click the **New Binding Rule** icon. The **Unbound Events Table** is displayed in its (start-of-session default) **Recommended Pattern** mode. To change the mode, click the **Tabular** or **Recommended Pattern** icon in the top right corner of the table. During a session, the system remembers and uses the last mode that was previously used.

Figure 161: Unbound Events Table in unexpanded recommended Pattern mode

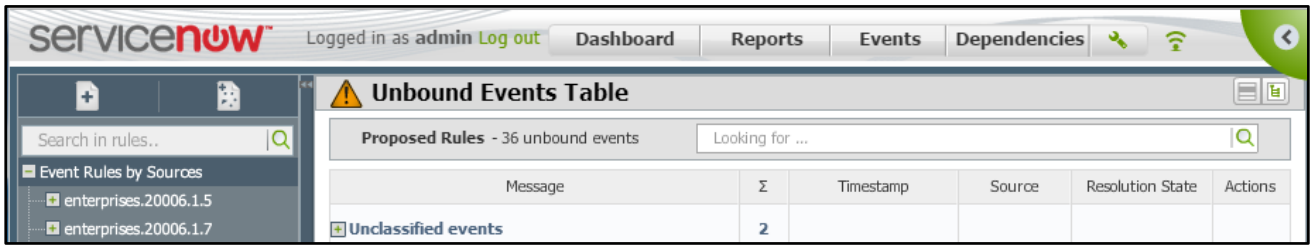
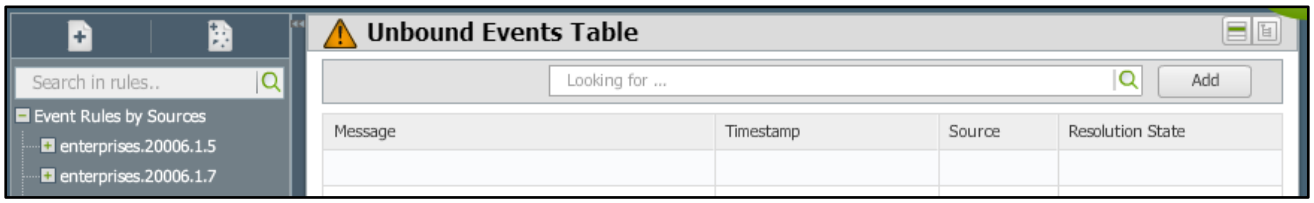


Figure 162: Unbound Events Table in Tabular mode



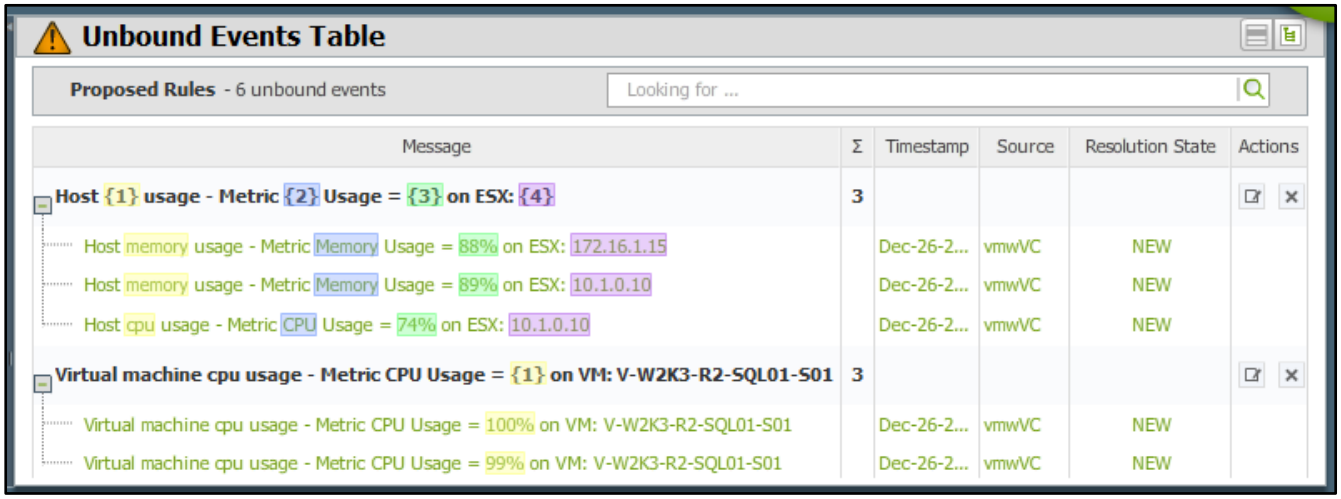
Tabular mode lists the **Message** text issued by the event, **Timestamp**, event **Source** (EMS), and **Resolution State** (e.g., NEW). In this mode, you can sort the **Unbound Events Table** on any column by clicking the header of that column. Clicking the header a second time reverses the sort order.

Notes:

- You can search for a particular value by entering the value in the Looking for search field.
- You can scroll forward and backward in the table using the vertical slide bar.
- You can display the details of an unbound event by right-clicking the event row and selecting Event Details from the pop-up menu. For more information, see Displaying the details of an event in the Unbound Events on page 180.

In **Recommended Pattern** mode, you can expand a bold message by clicking its icon to display up to 3 actual messages of that type. Click its icon to hide these messages.

Figure 163: Unbound Events Table in expanded Recommended Pattern mode



To define a new Binding Rule from the **Unbound Events Table**, you can

- double-click an event in the **Tabular** mode (Figure 162), *or*
- click the **Define Binding Rule** icon in the **Actions** column of a bold pattern group row in the **Recommended Pattern** mode (Figure 161 or Figure 163).

Note: If only one actual event is displayed in a pattern group, the **Define Binding Rule** icon will be on the non-bolded row of that actual event.

The New Binding Rule Definition screen will be displayed. See Figure 167.

Defining the Event Command Line

On Windows: The path for **nblevent.exe** is <ServiceWatch Server>\event_cli\bin\

On Unix: nblevent is a shell script in the path <ServiceWatch Server>/event_cli/bin/

To view the list of possible event fields, run <path>nblevent <URL>

Using the list of displayed event fields, create a command line that includes the desired fields. The following is an example of a command line: {▪

```
nblevent http://localhost:8080 emsSystem=test messageKey=22 emsEventID=12
severity=MAJOR text=”test message Severe Problem Detected" resolutionState=NEW
hostAddress=V-RHEL-5-32-WEB01.localhost.localdomain
```

Notes:

- On Unix machines, this utility uses **curl** or **wget** programs to send the http request.
- Command line options for **`nblevent`** on Unix and **`nblevent.exe`** on Windows are the same except for **`user`** (for basic authentication) on Unix. Configure the EMS to use this command line.
- In the current version of ServiceWatch, the `user` parameter and basic authentication should not be used. In a future release, this parameter will be supplied using the file ***`<ServiceWatch Server>`*`/event_cli/conf/`**

Mapping EMS Fields to ServiceWatch Fields

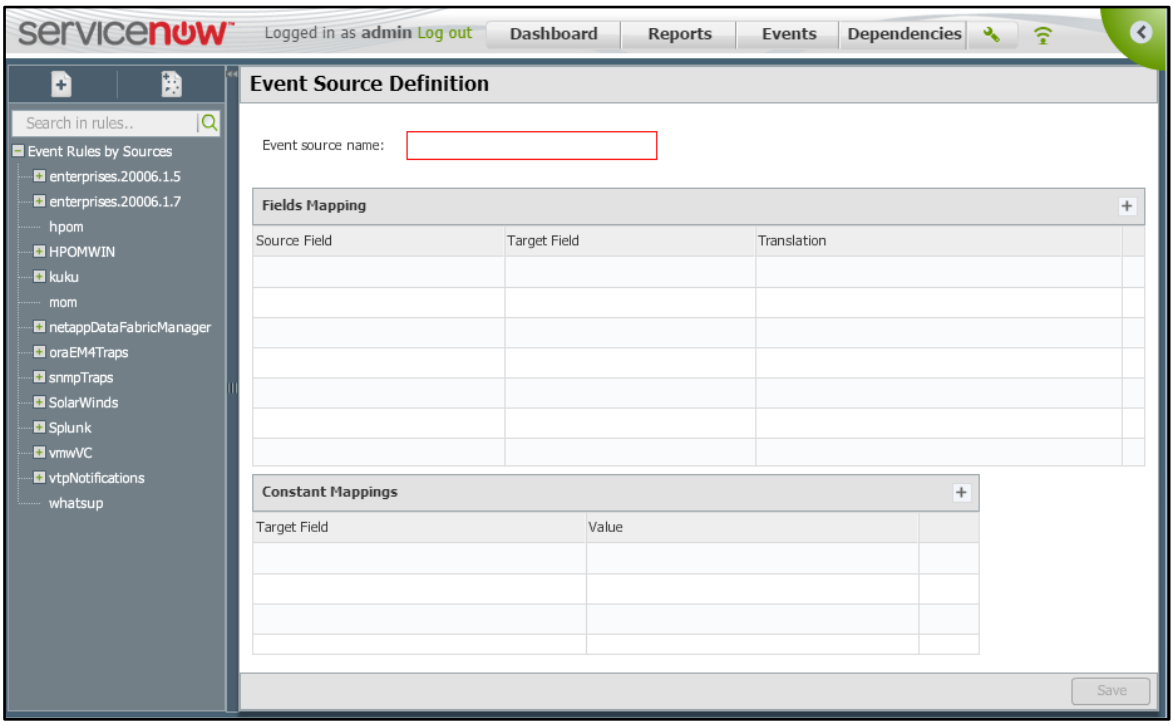
If EMS fields use different field names and/or values than those used by corresponding ServiceWatch fields, you must map the EMS field and its values to the corresponding ServiceWatch field and values. **vCenter** and **MOM** fields are already mapped in ServiceWatch. For other EMS applications, you must perform the mapping yourself.

For any EMS, you can optionally define constant values to be assigned to specified EMS fields by defining rules in the **Event Source Rules** screen. This screen contains two tables – the **Fields Mapping** table for mapping fields and values and the **Constant Mappings** table for defining constants.

To map EMS fields to ServiceWatch fields:

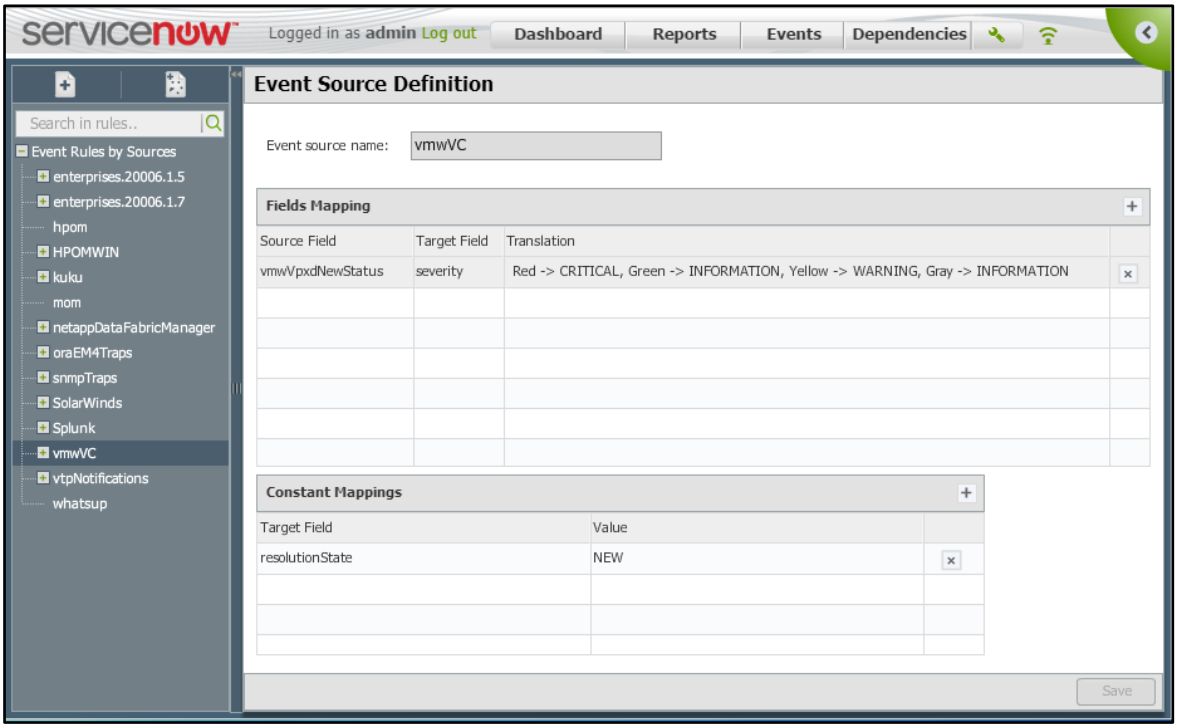
1. Click the Event Sources/Rules option of the  Settings drop-down menu.
2. Click the New Event Source  icon at the top of the Event Rules by Sources tree. An empty Event Source Definition window (Figure 164) is displayed.

Figure 164: Empty Event Source Definition screen



3. FIGURE 165 illustrates a rule for VMware's vCenter Server trap **vmwVC** in the **Event Source Definition** window.

Figure 165: Event Source Definition window with a rule

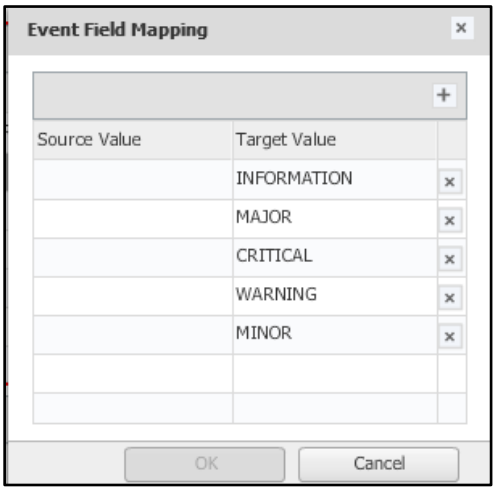


Note: To display or modify an existing Event Source Definition, click that definition (at level 1) in the **Event Rules by Sources** tree.

4. Select the (level 1) **Event source name** in the tree (for example, **vmwVC**). It is automatically inserted in the **Event source name** field.

5. Map EMS fields and values to ServiceWatch fields and values by doing the following for each EMS field to be mapped:
    a. Click the + button in the top right corner of the **Fields Mapping** table. A row opens to allow you to map the source field to the target field.
    b. The first value in the **Target Field** drop-down list is automatically entered in the **Target Field**.
    c. Click the **Source Field** to select or specify the name of the EMS field being mapped.
    d. Click the **Target Field** to select the corresponding ServiceWatch field from its drop-down list.
    e. Click the **Translation** field. The **Event Field Mapping** dialog box is displayed. It contains two columns: **Source Value** and **Target Value**. In some cases, the **Target Value** column is pre-populated with the ServiceWatch field values.

Figure 166: Event Field Mapping dialog box



    f. If the **Target Value** column is pre-populated, specify the corresponding EMS field values in the **Source Value** field. Otherwise, specify appropriate values in both columns. When finished, click the OK button. The **Source Value -> Target Value** pairs you specified are transferred to the **Translation** field.

6. To define constant values to replace EMS field values, do the following for each constant:
    a. Click the + button in the top right corner of the **Constant Mappings** table. A row opens to allow you to map a constant to an EMS field.
    b. In the **Target Field** column, specify the name of the EMS field that will be assigned the constant value.
    c. In the **Value** column, specify the constant value for that EMS field.

7. When you have finished the **Event Source Rules** definition, click the Save button. The event source rule is added to the system.

Extracting and Binding Event Information

This section contains the following topics:

Concepts

General

Binding rules are used to extract information from unbound events sent by the CLI (Command Line Interface) and to map that information either to object attributes or to new or existing event fields.

To define a new Binding rule, click the  button. The **Unbound Events Table** opens in (system default) **Recommended Pattern** mode (Figure 161) or **Tabular** mode (Figure 162).

In **Tabular** mode, you can either:

- define a new binding rule for an event in the table, *or*
- use the 

button to define a new binding rule for an event that is not in the table

In **Recommended Pattern** mode, you can click the  icon on a pattern row to define a new binding rule for an unbound event associated with that pattern. In either case, the **New Binding Rule Definition** screen (Figure 167) is displayed.

In **Recommended Pattern** mode *and* when you select an event in the **Unbound Events** table in **Tabular** mode, the **New Binding Rule Definition** screen is pre-populated with source fields and values taken from the event.

When defining a Binding rule in **Tabular** mode for an event that is not in the **Unbound Events** table, source fields and values are not pre-populated and you must supply all of the required data.

Mapping Logic

ServiceWatch searches for the appropriate rule so that it can determine which target values to substitute for event source values. The value(s) from an **Event source** field can be one or more variables, a constant, or one or more variables with a constant.

Note: In this discussion, the term 'variable' is simply the content of an event source field that can vary. The term 'constant' is the content of (a part of) an event source field that cannot vary.

- If an Event source field contains a mix of variables with or without a constant, you can make multiple extracts from the source field and provide an appropriate **Target**, **Field** and **Assigned Value** for each extract.
- If an Event source field consists of only one variable *or* only a constant, finding the appropriate transformation rule is easy.

- If the field contains a mix of variables with a constant, finding the appropriate rule is more difficult. ServiceWatch looks at the constant as well as the variables to find the appropriate rule.

How you treat source values in the **Event Fields Rules** table and **Advanced Rule Binding Definition** table impacts the results of the search mechanism. When mapping source values, follow these guidelines:

- If the entire source value is one variable, leave it unmapped and the algorithm will treat the value like a variable.
- If the entire source value is a constant, click the **Constant** column for that row and select the checkbox that is displayed on that row.
- If the value consists of any combination of variables with or without a constant, leave the constant (if any) unmapped.
- Map every variable separately. If you have mapped at least one variable, the algorithm treats the unmapped portion as a constant.

Define the Binding Rule for an Event

1. Display the Unbound Events Table

   a. Click the **Event/Sources Rules** option of the  **Settings** drop-down menu in the dashboard.

   b. Above the tree pane, click the New Binding Rule  icon. The **Unbound Events Table** opens in **Recommended Pattern** mode (Figure 161) or **Tabular** mode (Figure 162).

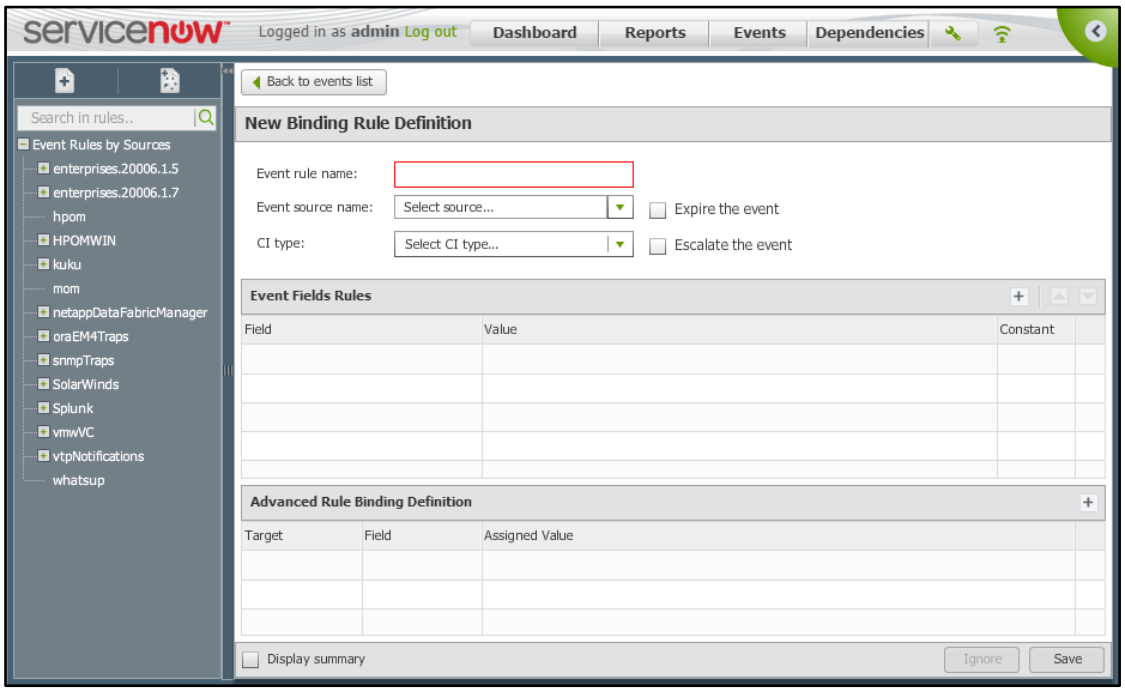
Notes:

- To search for an event in either mode, enter a search string in the Looking for **Search** field above the table.
- You can scroll up or down in either mode by using the vertical slide bar.
- In either mode, you can display the details of an unbound event by right-clicking the event row and selecting Event Details from the pop-up menu. For more information, see DISPLAYING THE DETAILS OF AN EVENT IN THE UNBOUND EVENTS on page 180.

2. Begin defining a Binding rule by doing any of the following:
   - ✓ To define a Binding rule for unbound events that match a pattern listed in Recommended Pattern mode, click the  icon for that pattern.
   - ✓ To define a Binding rule for a specific unbound event, find that event in Tabular mode and double-click its row in the table.
   - ✓ To define a Binding rule from scratch, use Tabular mode and click the 

button.
3. In each case, the same **New Binding Rule Definition** screen (Figure 167) is displayed.

Figure 167: New Binding Rule Definition screen



Notes:

- The top of the screen contains fields for defining general details about the rule such as Event rule name, Event source name, and CI type. You must fill or select a value for these fields before doing anything else in this screen.
- To set expiration criteria, click the **Expire the event** checkbox. In the displayed **Hours** and **Minutes** fields, select the time interval after which the event will expire (that is, be closed). As a practical matter, the expiration interval should not be less than or equal to the escalation interval.
- To set escalation criteria, click the **Escalate the event** checkbox. In the displayed **Hours** and **Minutes** fields, select the repetitive time interval after which the event status will escalate to the next higher level. For example, if you set the time interval to 1 hour for an event whose status is Minor, after one hour its status will escalate to Major and after another hour its status will escalate to Critical.
- The middle portion of the screen contains the **Event fields rules** table which will usually contain pre-populated **Field** = **Value** rows. If there is absolutely no variable text on a row, click the **Const** column to insert a check-mark in that row.
  In most cases, the text field and its value are the most important row in this table because the value in this row is most likely to contain the constant and/or variable values that identify the CI to which the event should be bound.
- The bottom portion of the screen contains the **Advanced Rule Binding Definition** table with **Target**, **Field**, and **Assigned Value** fields.

  Both tables have [+] buttons for specifying additional Field = Value or Assigned Value pairs.

4. You can add, modify or delete values in the Event Fields Rules table. For instructions, see Defining rows in the Event Fields Rules table.
5. Add, modify or delete values in the Advanced Rule Binding Definition table. For instructions, see Defining rows in the Advanced Rule Binding Definition table.

6. If you reach the **New Binding Rule Definition** screen while in **Tabular** mode, click Save when finished to cause messages that match the definition to be bound to the appropriate configuration item.

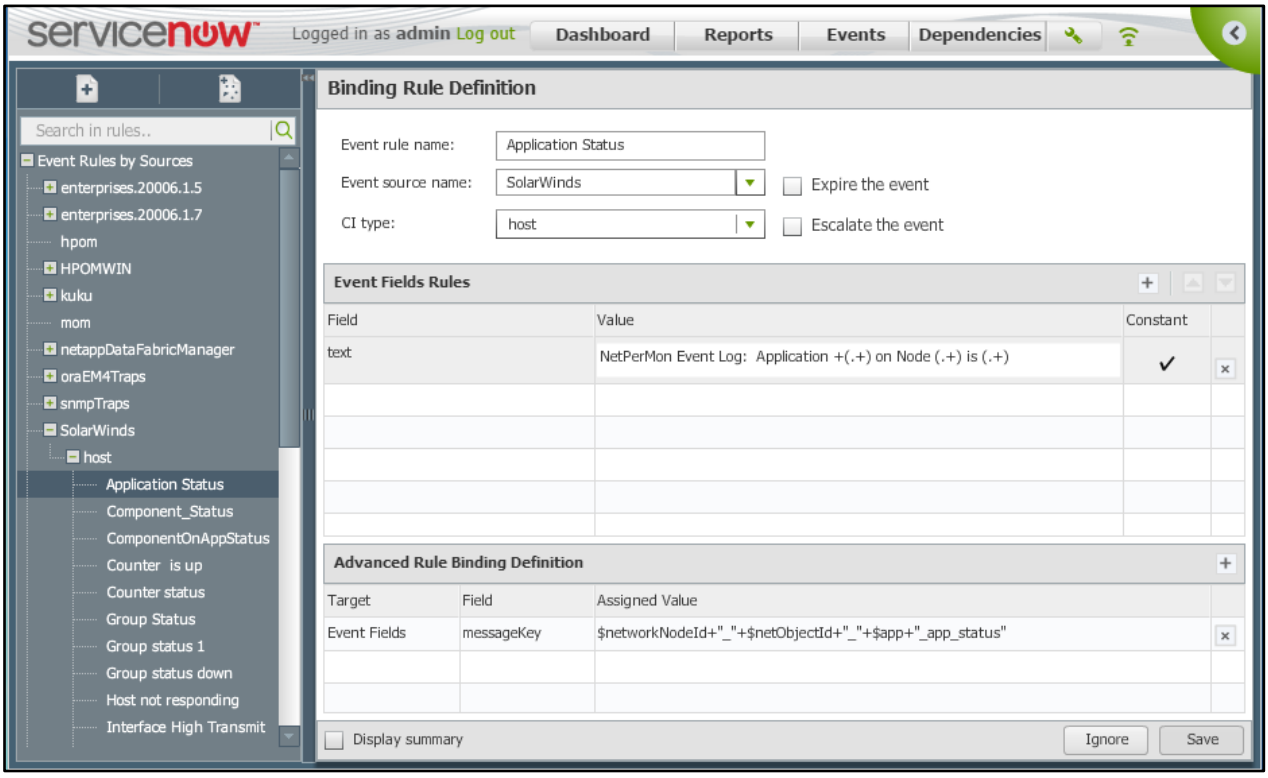
   Click Ignore to cause messages that match the definition to be ignored and discarded.

7. If you reached the **New Binding Rule Definition** screen while working in **Recommended Pattern** mode, click Skip to leave the event unbound or click Ignore to cause messages that match the definition to be ignored and permanently discarded. If you click Next, the specified rule will be applied to ***all*** of the unbound events associated with the current pattern, if possible. An existing unbound event (if any) that matches the *next* pattern in the **Unbound Events Table** will be displayed.

Defining rows in the Event Fields Rules table

The **Event Fields Rules** table lets you identify and extract all or part of the source event field and map the extract to CI attributes. Each row in the table represents data provided by the event source. FIGURE 168 illustrates an existing **Binding Rule Definition** screen that is already filled in.

Figure 168: Binding Rule Definition



Notes:

- The Event Fields Rules table contains **Field**, **Value** and **Constant** columns plus a delete row icon. This table is used when the received Field name may need to be (and usually is) changed in the Target/Field dialog box but the received Value is passed to the target field unchanged. If this Value must be changed, then the Advanced Rule Binding Definition table at the bottom of the screen must be used to specify the target value in the Assigned Value column. The Advanced Rule Binding Definition table is also used to concatenate a combination of values.

- The **Field** and **Value** columns identify source fields. Each source field has its own row in the table. If you are defining a rule for an existing unbound event, these fields are populated with information from the event.
- Holding the hand-cursor over a constant or variable in the Value column displays a tool tip.
- Selecting all of a variable value or part or all of a constant in the **Value** column causes the **Target/Field** dialog box (Figure 169) to be displayed. This dialog box contains **Target** and **Field** columns for setting ServiceWatch values that are equivalent to source event values.
- If a selected value (or part of a value) is a constant, click in the **Constant** column for that row. It will change to ☑ .

1. To fill in a new Binding Rule Definition from scratch (for an unbound event that does not currently exist), specify the **Field** and **Value** data in the **Event Fields Rules** table as follows:

   b. Click the **+** button in the header of the **Event Fields Rules** table to add an empty row.

   c. In the **Field** column, specify the field type.

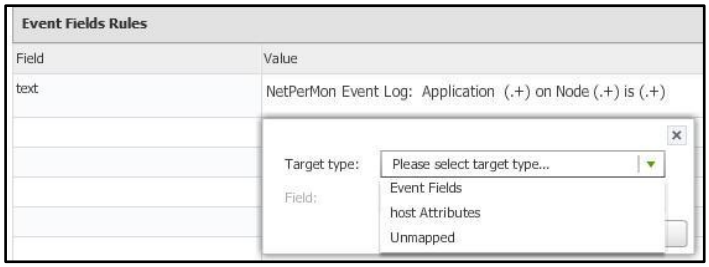
   d. In the **Value** column, specify the value to be returned by the event.

   e. Repeat steps 1.a, b and c for each **Field** = **Value** row that is required to identify the unbound event.

2. Perform the following sub-steps for each **Field** = **Value** row (whether pre-populated or specified in step 1) for which a ServiceWatch **Target** and **Value** are required:

   a. Select all of a variable value or part or all of a constant in the **Value** column. The **Target type** dialog box is displayed.

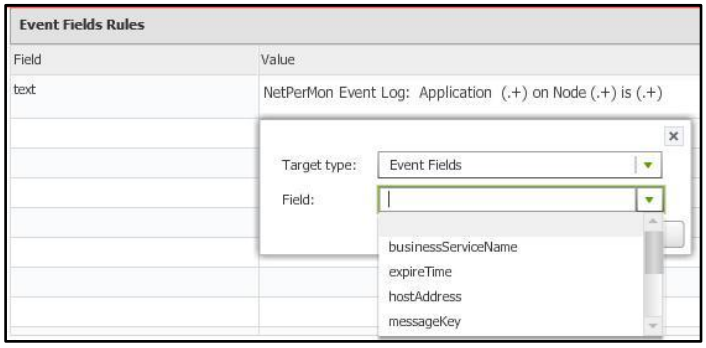
Figure 169: Target type/Field drop-down list



   b. Select the **Target type** from its drop-down list.

   c. Select the **Field** value (if any) from its drop-down list.

Figure 170: Field value drop-down list



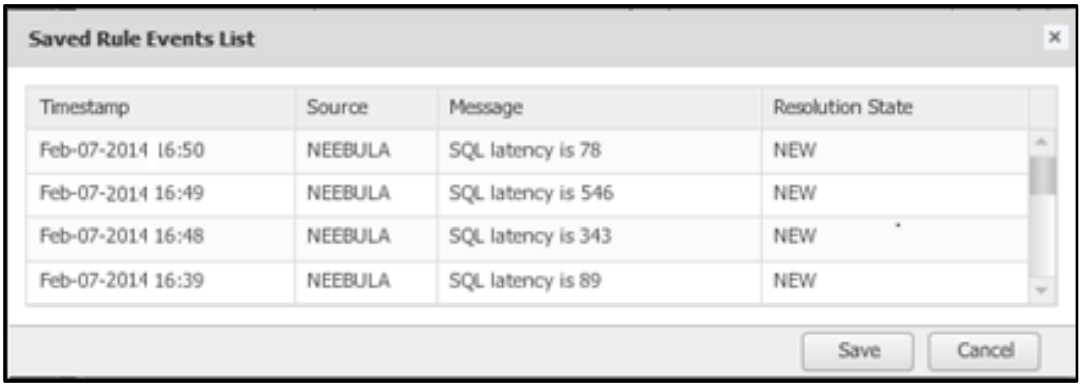
   d. Click the OK button. The selected string will be assigned to the specified target field.

3. For each row handled in step 2, perform this step whether you are creating a Binding Rule Definition from scratch or for an existing unbound event.
   - ✓ If the entire value in the **Value** field is a constant, click the Const column and skip step 4.
   - ✓ If the entire value in the **Value** field is a variable, skip step 4.
   - ✓ If the **Value** field contains at least one variable *plus* other variables or constants, perform step 4.
4. Do the following for each variable string in the **Value** field:
   a. Select the variable text string. The **Target type/Field** dialog box is displayed. Values in the **Field** drop-down list vary according to the value selected in the **Target type** drop-down list.
   b. Map the selected string by doing one of the following:
      - If the selected string identifies an attribute (property) of the CI type that you specified above the table:
        i. In the **Target type** drop-down list, select **<CI> Attributes**.
        ii. Select the relevant CI attribute in the **Field** drop-down list.
   c. If the extract should *not* be linked to a specific field or attribute (or if the variable is not important), select **Unmapped** as the **Target type** value. No **Field** drop-down list will appear. (Example: The extract ORA can indicate that the rule relates to Oracle, but the extract does not relate to a specific field or attribute.)
      - If the extract provides other information about the event:
        i. In the **Target type** drop-down list, select **Event Fields**.
        ii. Select the relevant ServiceWatch field in the **Field** drop-down list.

Note: Be sure to map all variable strings and leave all constants unmapped.

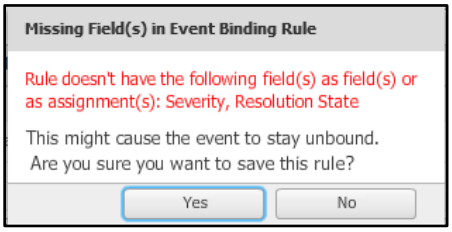
5. After you finish steps 2 through 4, perform the steps described in Defining rows in the Advanced Rule Binding Definition table on page 179 if and only if one or more target fields specified in steps 2 through 4 must be changed to a value other than the **Value** displayed in the **Event Fields Rules** table.
6. If you select the **Display summary** checkbox at the bottom of the screen, the saved rules (if any) that apply to that type of event will be automatically displayed in the **Saved Rule Events List** (Figure 171).

Figure 171: Saved Rule Events List



7. When you finish handling the relevant rows in the **Event Fields Rules** table and, if necessary, in the **Advanced Rule Binding Definition** table, click the Save or Ignore button in **Tabular** mode, *or* the Ignore
8. If expected fields are missing, the **Missing Fields** confirmation box is displayed.

Figure 172: Missing Field(s) confirmation box



9. In **Recommended Pattern** mode, the specified rule is applied to ***all*** of the unbound events associated with the current pattern, if possible, and an existing unbound event (if any) that matches the *next* pattern in the **Unbound Events Table** will be displayed.

Defining rows in the Advanced Rule Binding Definition table

This table enables you to assign any value to a ServiceWatch target field. The Assigned Value can be a simple value or a complex value that includes concatenations and expressions. See Figure 168 for an example of an Advanced Rule Binding Definition filled-in table row.

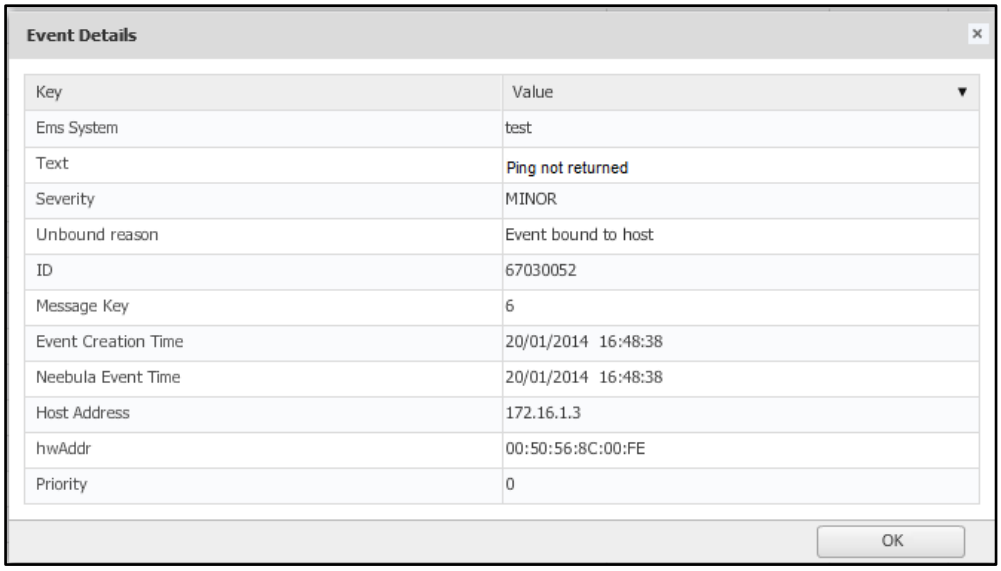
1. Perform these steps for each target field value to be assigned:
   a. Click the + button to add a row to the table.
   b. From the **Target** drop-down list, select the value (**Event Fields** or **<CI type> Attributes**) that is appropriate for the selected **CI type** near the top of the screen.
   c. From the **Field** drop-down list, select the field for which you are defining the value. The values available in the **Field** drop-down list vary according to the selected **Target** value.
   d. Specify the **Assigned Value** for that field.
2. When you finish handling the relevant rows in both the **Event Fields Rules** table and the **Advanced Rule Binding Definition** table, click Save or Ignore in **Tabular** mode or click Skip, Ignore
3. In Recommended Pattern mode, the specified rule will be applied to all of the unbound events associated with the current pattern, if possible, and an existing unbound event (if any) that matches the next pattern in the Unbound Events Table will be displayed.

Displaying the details of an event in the Unbound Events Table

1. Click the New Binding Rules icon to display the **Unbound Events Table**.
2. If the table is not already in **Tabular** mode, click the **Tabular** icon in the top right corner of the table. See Figure 162.
3. Find the row of the event whose details you want to display and right-click that row. In the pop-up menu, select the **Event Details** option. The **Event Details** table displays information about that event (Figure 173). You can sort this table by clicking **Key** or **Value** in the header row. Click again to reverse the sort sequence.
4. When you finish viewing the details, click OK to close the **Event Details** table.

Note: Event details can also be displayed by right-clicking an event that is displayed in the **Unbound Events** table in *expanded* **Recommended Pattern** mode (Figure 163). However, only a few events in each pattern are displayed.

Figure 173: Event Details table



For an alternative method of displaying Event details, see Figure 33 on page 52.

Table 1 on page 53 describes the Keys that may be listed in the **Event Details** window.

Chapter 8: Monitoring Business Services

This chapter contains the following topics:

Concepts

After a business service skeleton is defined and activated, ServiceWatch generates a continuously updated topology that it uses to monitor the business service in real-time.

In the Monitoring window, ServiceWatch displays color-coded graphic representations of your business services statuses. You can determine at a glance the priority of all business services and the severity of any problems that the services might have.

Using this information, you can determine which business service should be examined and then display the details of that business service by clicking its node in the **Active** tree in the left panel or double-clicking its tile or bubble in the **Monitoring** screen.

In the bottom pane, the **Monitoring** screen displays relevant information in the **Events** panel.

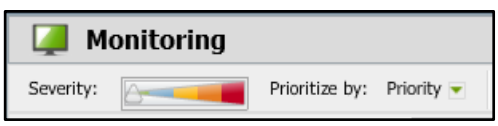
Note: The bottom pane also has a KPI (Key Performance Indicators) panel. This panel is discussed in KPIs (Key Performance Indicators) on page 194.

Using the details that ServiceWatch provides in the Dashboard and **Monitoring** window, you can take the necessary actions required to keep your business services up and running.

Severity Color Coding

The color coding identifies the severity of the problem:

- CRITICAL
- MAJOR
- MINOR
- WARNING
- INFORMATION



The business service is color coded according its most severe event. For example, if a business service has a Critical event and Minor event, it is color coded as Critical. To filter the business services that are displayed in the Dashboard by severity, use the **Severity** slide near the top left corner of the Dashboard. Business services whose severity code color is located to the right of the slide will be displayed.

Event Priority

The priority of an event is displayed as a number from 0 - 100. Higher numbers indicate higher priority. Event priority is automatically calculated by a proprietary algorithm that evaluates

- the extent to which an event affects a business service
- the severity level of that business service caused by the event
- the number of business services affected by the event

Viewing All Business Service Statuses at a Glance

To view the overall situation of all business services at a glance:

1. Select 

and expand the **Active** tree in the left panel. The Dashboard is displayed in its current format: **Tile** (Figure 174), **Bubble** (Figure 175) or **List** (Figure 28).
2. For information about Dashboard formats, see Dashboards on page 42.

Tile Dashboard

In this Dashboard, the tiles are arranged by configured groups, their size indicates their relative priority or importance, and they are colored according to their severity level.

Figure 174: Tile Dashboard

Bubble Dashboard

In this Dashboard, the bubbles are usually arranged vertically by priority and horizontally by severity. Therefore, the business services that require the most immediate attention are located in the top right (shaded) area of the Dashboard.

Figure 175: Bubble Dashboard

List Dashboard

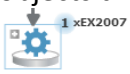
For information about this Dashboard, see List Format Dashboard on page 48.

View a Business Service or CI

To view a business service or CI's status, details, and Events or KPIs:

- Click its node in the **Active** tree, *or*
- Double-click its tile in the Tile Dashboard, *or*
- Hover over its bubble in the Bubble Dashboard and click See topology in its tool tip.

Figure 176: Bubble tool tip

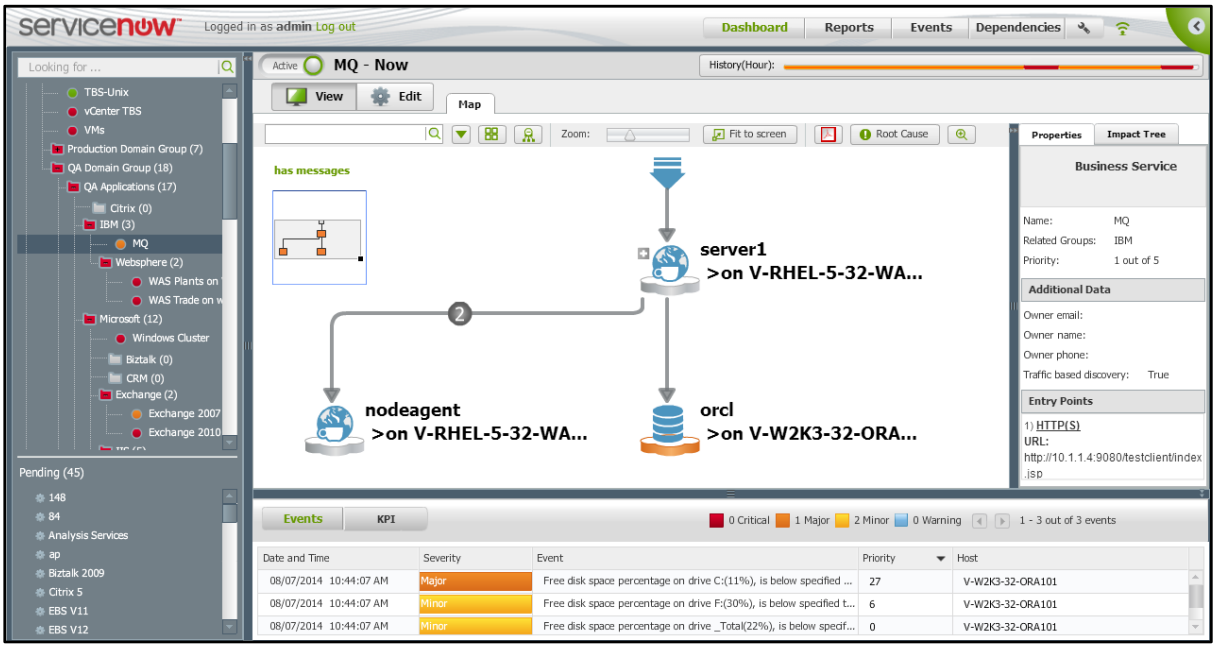
1. The Dashboard (Figure 177) displays topology of the selected business service or CI. Topology objects that constitute a Cluster are surrounded by a blue box, for example, 

. You can right-click the blue box to display the CIs in it surrounded by a red box.
2. If a business service or CI is already displayed in **Edit** mode, click the 

button.

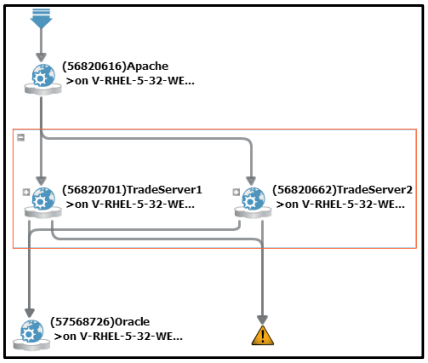
Map Panel

Figure 177: Topology Map in View mode



- The map displays all the components of business service that were discovered.
- The color of the plate under each CI indicates its severity level.

- Click a CI to display its properties, events, impact tree, and KPIs (if any). Click the topology background to return to the business service level.
- To determine the status of a connection, right-click its network or storage path.
- You can format the topology display. See ADJUSTING THE TOPOLOGY MAP on page 162.
- To change or fix the topology, click Edit. For details, see ADJUSTING THE BUSINESS SERVICE TOPOLOGY on page 138.
- The impact status of events on a business service is displayed in the right pane.
- To view the properties of a business service, object or connection, select the business service or object, or click the connection. The properties are displayed in the pane on the right (see BUSINESS SERVICE, OBJECT OR CONNECTION on page 157).
- To display an object's events in the bottom pane, select the object in View mode. To display all events of a business service, click anywhere in the blank space of its topology.
- To display details of an event in a pop-up table, double-click that event in the bottom pane. Sort the table's rows by clicking the Key or Value header. Click again to reverse the sort.
- indicates ServiceWatch does not know what happened to the server (e.g., the server is down).
- The **Events** pane does not list events with a severity status of **Information**.
- CIs that constitute a Cluster are surrounded by a **red** rectangle, for example,



- To display hosts (and host connections) instead of the applications running on them, click the icon. It will become grayed-out. Click it again to redisplay the applications.
- To return to the top level of the Dashboard, click Dashboard or the **Active** tree root.

Modifying Monitor Attributes

ServiceWatch uses built-in and user-defined Group & Business Service Monitors (page 86), Aggregate Monitors (page 187) and (User Experience) Synthetic Monitors (page 188).

The monitors can be enabled/disabled and the dates and times when the monitors are operational can be scheduled. There are two scheduling options. Basic scheduling causes monitors to run every *x* minutes. Advanced scheduling enables monitors to run *y* times a day during specified time intervals.

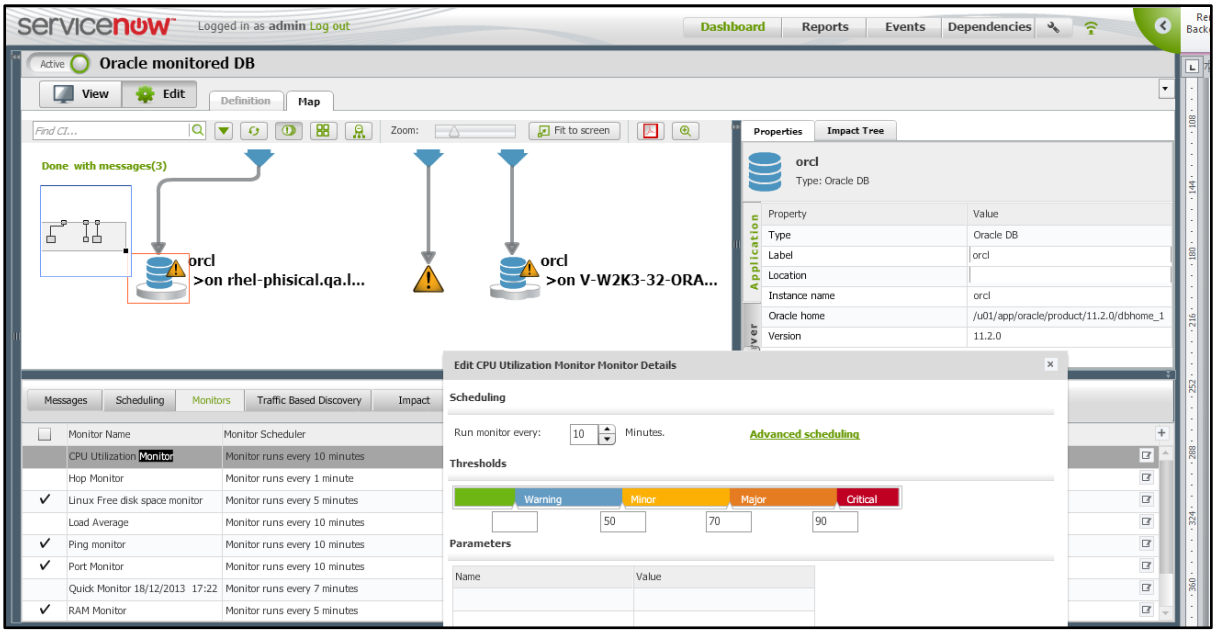
To view, set or change monitor criteria, click  and click the **Group & Business Service Monitors** link in the **Settings** menu.

Figure 178: All Groups & Business Services tree

In the **All Groups & Business Services** tree, locate the CI whose monitor attributes you want to examine or modify. In this example, we located the **Oracle monitored DB**.

In the **Dashboard > Active** tree, select that CI to display its topology Map. To change the frequency or the severity criteria of that CI's monitor, select that CI in the topology Map, click the **Monitors** tab in the bottom pane, and double-click the monitor you want to edit in the table of monitors. The **Edit <monitor name> Monitor Details** dialog box enables you to fine-tune that monitor.

Figure 179: Typical Monitor Modification screen



For information about scheduling, see Figure 195: Edit Monitor Scheduler dialog box on page 195.

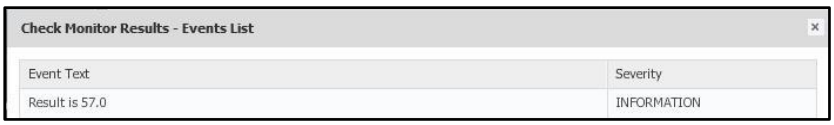
Make the desired changes, if any, and click 

.

Click 

to generate monitor output, for example:

Figure 180: Check Monitor Results – Events List



Click 

to exit without saving changes. Click 

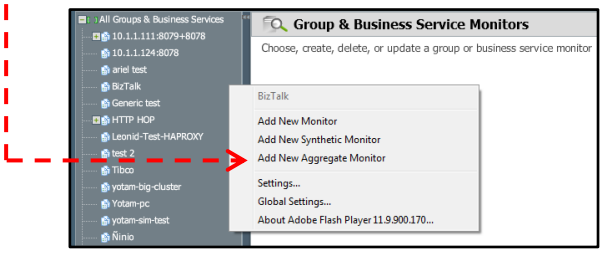
to delete the monitor.

Aggregate Monitors

An *aggregate* monitor enables you to monitor the performance of a collection of CIs in a Group or a Business Service as a unit. It combines the results of similar monitors and enables you to view the combined output of those monitors. The output can represent the sum, average, minimum or maximum amount of the performance being monitored. For example, you can sum a group of sales monitors to display total sales for a time period.

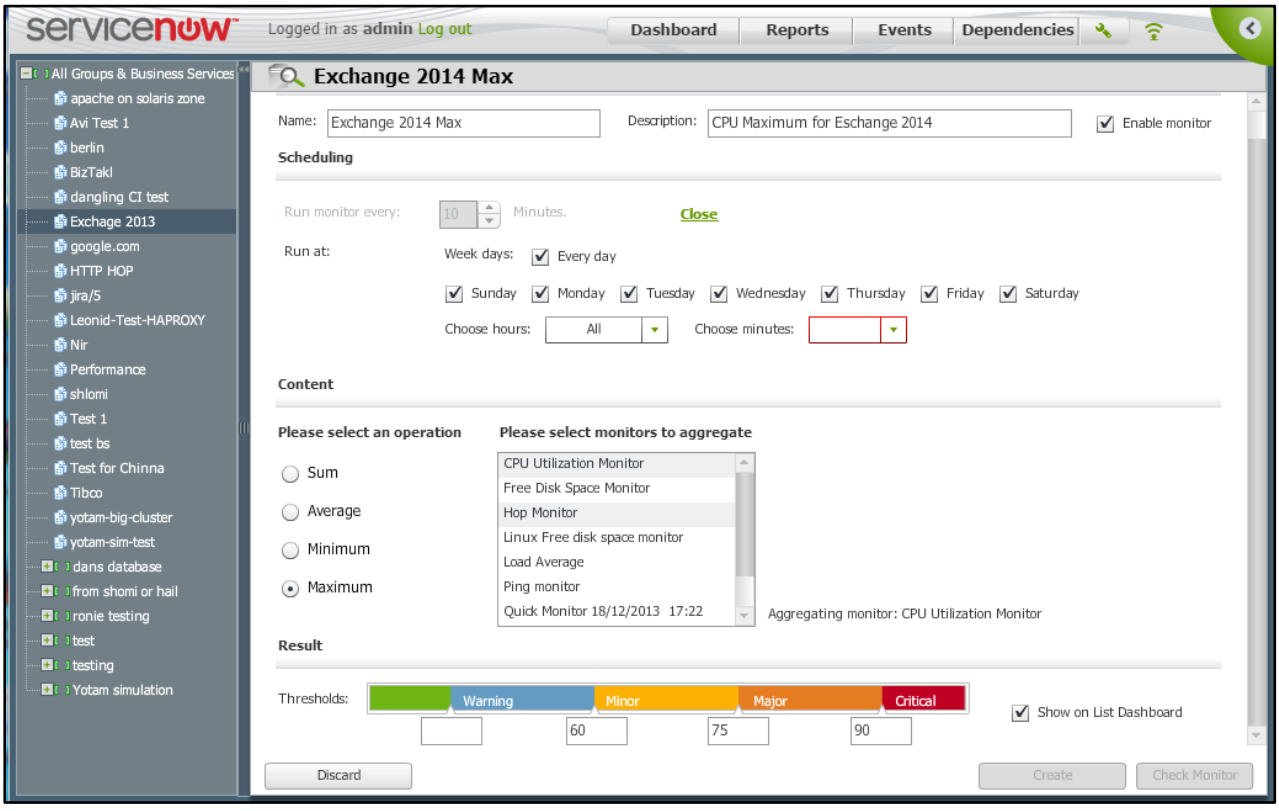
To add an aggregate monitor to a Group or Business Service, click  , click the **Group & Business Service Monitors** option, right-click a Group or Business Service in the tree, and select the **Add New Aggregate Monitor** option in the pop-up menu.

Figure 181: Add New Aggregate Monitor option



A screen similar to the **Monitor Modification** screen in Figure 179 is displayed.

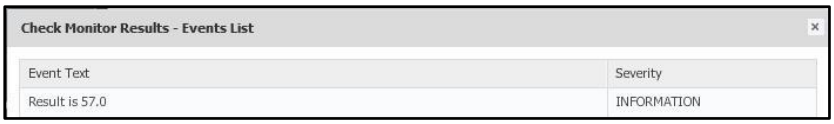
Figure 182: Add a new Aggregate Monitor screen



Click  to save the new aggregate monitor.

Click Check Monitor to generate monitor output, for example:

Figure 183: Check Monitor Results – Events List



Click Cancel to exit without creating or saving changes.

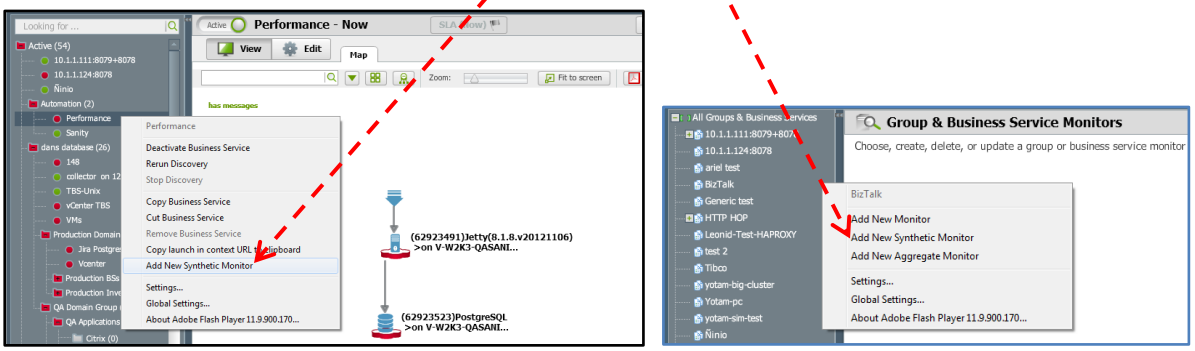
Click Delete to delete an existing aggregate monitor.

Synthetic Monitors

Synthetic (user experience) monitors enable you to monitor the performance of an entire business service from the user's perspective. It records the essential sequence of transactions that are performed when using a business service via the web application, then re-plays those transactions periodically while measuring the validity of each transaction, the total time required for the entire sequence, and the overall level of success obtained.

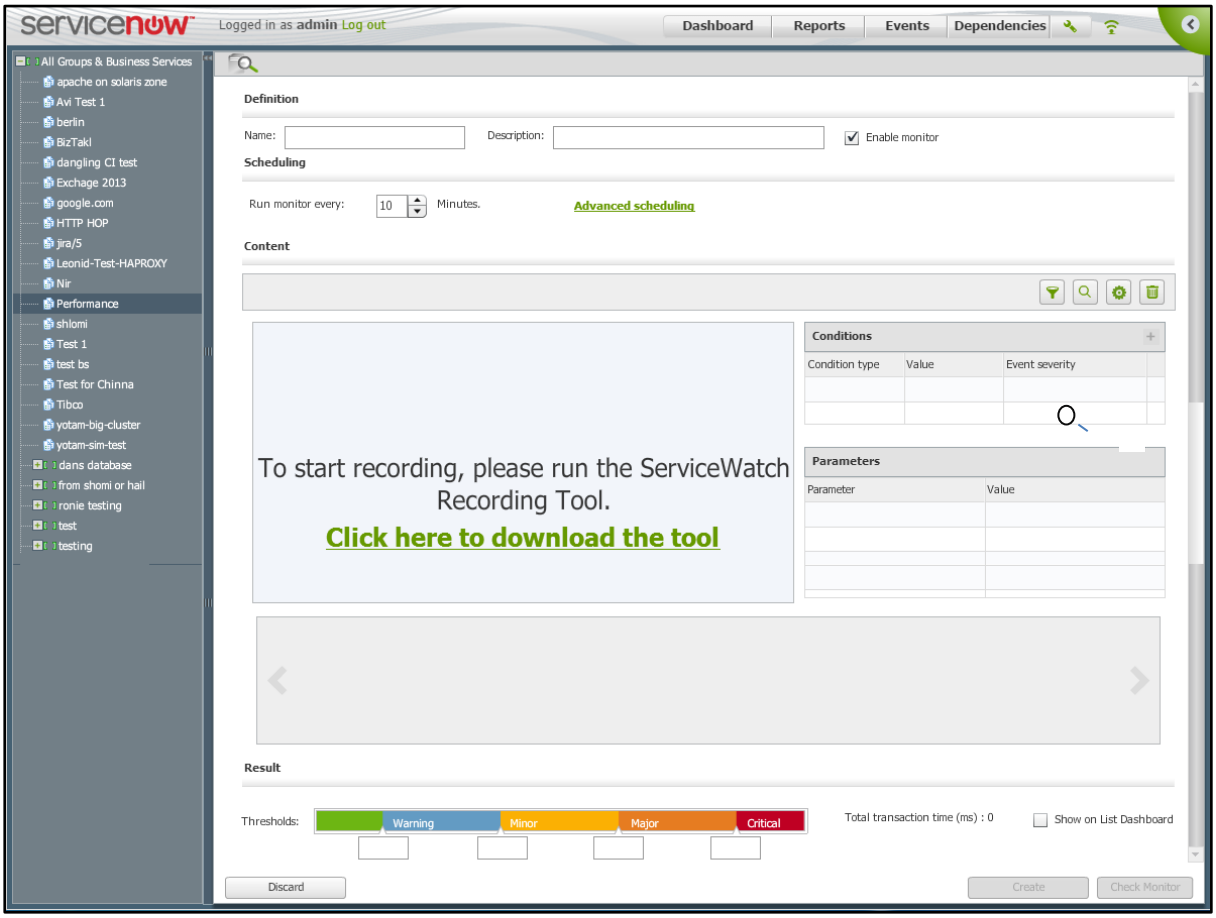
To add a synthetic monitor to a business service, right-click that business service in the **Active** or **Pending** Dashboard tree and select the **Add New Synthetic Monitor** option in the pop-up menu *or* click , click the **Group & Business Service Monitors** option, right-click a Business Service in the tree, and select the **Add New Synthetic Monitor** option in the pop-up menu.

Figure 184: Add New Synthetic Monitor option



The screen in Figure 185 is displayed.

Figure 185: Add a new Synthetic Monitor screen



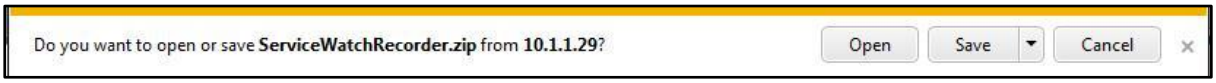
Enter a **Name** and **Description** for the monitor, use the up or down arrows to specify how often it should run (**Frequency** in minutes), and verify that the **Enable monitor** checkbox has been selected.

Recording Tool

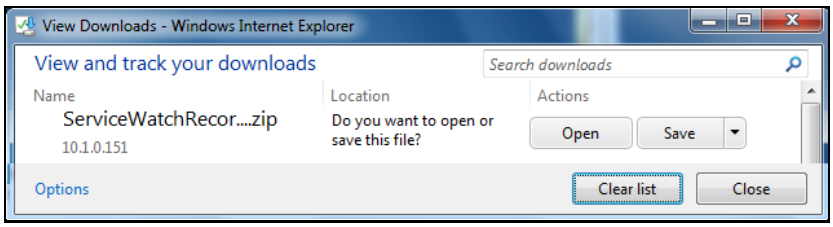
Click the Recording Tool link (Click here to download the tool) only once for each ServiceWatch client machine to download a zip file containing a **MinHook.x86.dll** file, a **params.ini** file and a **ServiceWatchRecorder.exe** file. Different download dialog boxes are displayed by Internet Explorer (IE), Chrome and Firefox.

Downloading

For example, the download box may look like this:



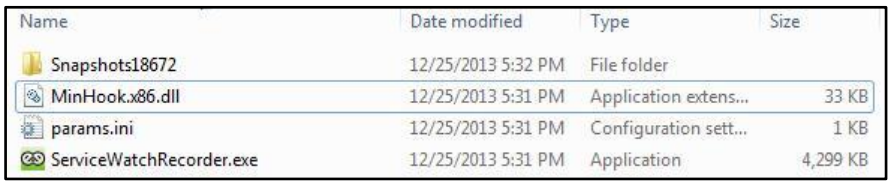
or this:



Installing

Extract and save these files in the same folder in a location that is accessible from the ServiceWatch client machine. Make a note of this folder's path or save it on the desktop. When using an IE browser, this folder's contents are displayed like this:

Figure 186: Files extracted from ServiceWatchRecorder.zip

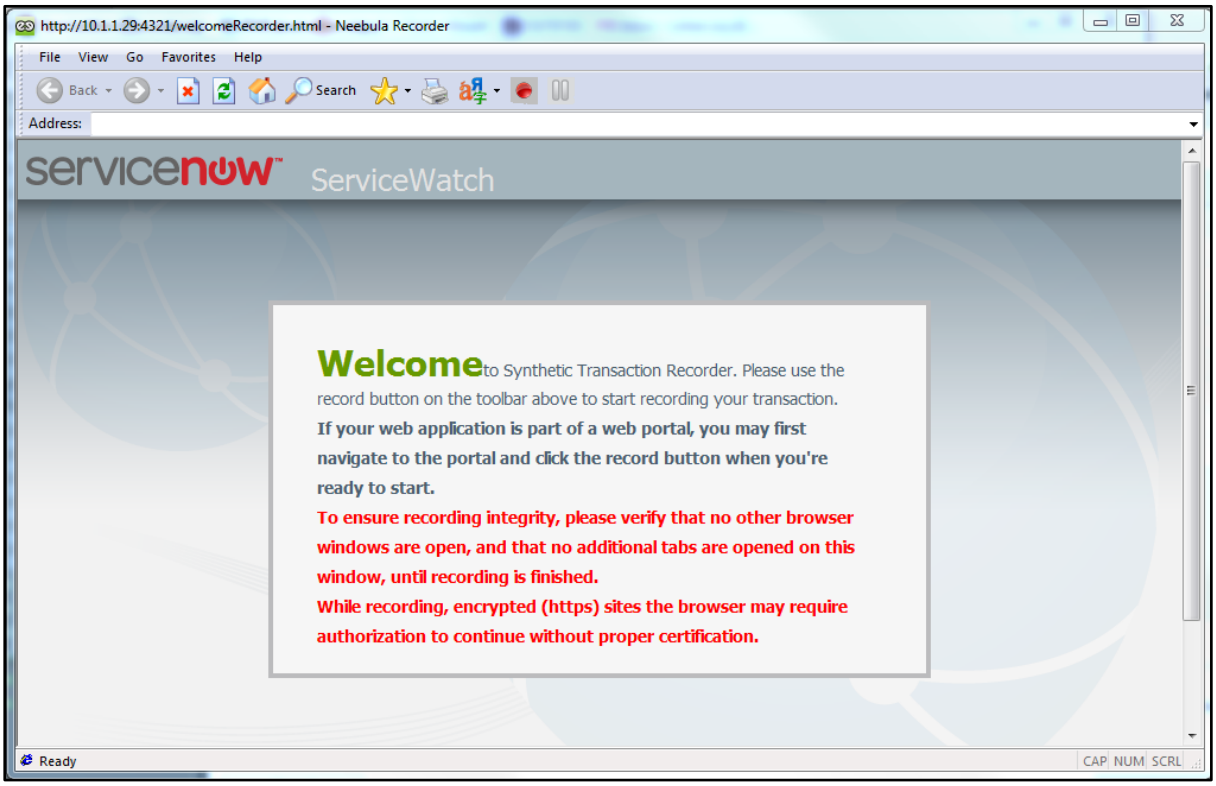


The collector (and its proxy) must also be accessible from the same client machine.

Before recording the transactions with a Synthetic (user experience) monitor, you should close all other currently running applications except ServiceWatch. Do *not* close ServiceWatch while recording because there is continuous communication between the recording tool and ServiceWatch during the recording process.

Run **ServiceWatchRecorder.exe** to display the Synthetic Transaction Recorder's Welcome screen in a new automatically opened **Internet Explorer** browser instance. This is the only browser instance that can be used for recording.

Figure 187: Synthetic Transaction Recorder wizard's Welcome screen



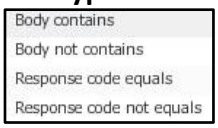
Recording

Start recording by clicking the red dot Start button  . The Start button  turns **grey** and the Stop button  turns **green**, indicating that recording is in progress. To stop recording, click the Stop button  (which turns **grey**). Pause recording by clicking the **green** pause button.

Recording the business service transaction automatically populates the **Content**, **Conditions**, and **Parameters** areas of the **Add a New Synthetic Transaction Recorder** screen. For example:

Figure 188: Content, Conditions & Parameters of the Synthetic Transaction Recorder wizard

A thumbnail of each transaction screen is located at the bottom of the **Content** area. Clicking a thumbnail displays the **Conditions** and **Parameters** (if any) associated with that transaction.

The **Conditions** panel lets you assign **Event severity** levels to **Condition types** whose value exceeds the **Value** you specify. The available **Conditions types** are: 

.

Click  to open an input row. Use the down arrow to select the **Condition type** (default: **Body contains**) from its drop-down list. In the value column, specify a text string or response code whose presence or absence causes an **Event severity** to be applied to that transaction. Click the **Event severity** column (default: CRITICAL) and click its down-arrow to select the severity level that will be applied. The severity level of the monitor is the most severe level applied to any of its transactions. Click  in the right column of a row to delete that row.

The **Parameters** panel displays the current **Value** of each **Parameter** that exists in a transaction and lets you change that value.

Parameters and their current values are automatically populated in transactions that have parameters. If you click a value, it becomes highlighted and can be changed. Parameter names cannot be changed.

Click the **Parameter** or **Value** heading to sort the **Parameters** panel. Click the same heading again to reverse the sort.

When creating the monitor, the **Total transaction time** (in milliseconds) is automatically recorded In the **Result** area. You can enter values (also in milliseconds) in any or all of the 4 empty boxes to specify thresholds above which the indicated severity level is applied to the business service.

Figure 189: Total transaction time and Threshold levels in milliseconds

There are 4 special buttons  at the top right corner of the **Content** area.

The  button lets you specify file extensions to be skipped but it does *not* delete URLs with these extensions from the **Content** area. For example, specifying ***.png** will filter out .png URLs. After such URLs have been specified, clicking the  button displays the specified extensions to be filtered. Placing the cursor in the text box displays a  button that can be clicked to delete its extension.

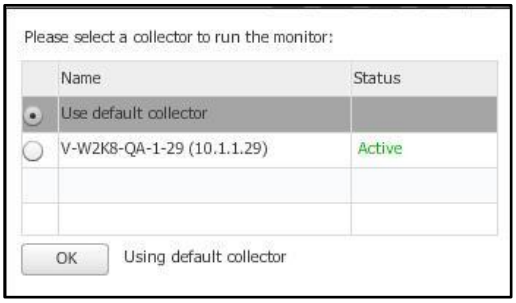
Figure 190: File extension deletion button

The  Search button highlights parameters that contain a specified value. Clicking the  button again highlights the next occurrence of that value. After the last occurrence has been displayed, clicking this button will re-display the first occurrence.

Figure 191: Search for next-occurrence button

When more than one collector can be used with a Synthetic (user experience) monitor, the  button enables you to select the collector that will be used. For example:

Figure 192: Select a Collector dialog box



The  button deletes all transactions from the **Content** area. It does *not* delete the monitor. This button is useful when you want to monitor the transactions after making changes to the business service that is being monitored.

Caution: This button also deletes existing **Conditions** and **Parameters** specifications.

Click 

to save the currently displayed Synthetic monitor.

Click 

to delete the currently displayed Synthetic monitor.

Click 

to exit this screen without saving the monitor (or changes made to it).

Click 

to run the currently displayed monitor immediately.

KPIs (Key Performance Indicators)

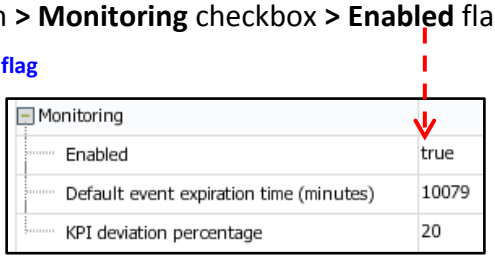
KPIs can be based on *any* integer or floating point number that is meaningful for the user. Obvious examples are CPU usage and percentage of used or unused storage. Less obvious examples are the value of sales or number of customer service tickets per unit of time.

Each KPI is associated with an active monitor. Therefore, KPIs can be viewed per business service, per group, etc.

Settings

In order to generate KPI thumbnail graphs or tables, ensure that the  > **Settings** menu **> Global Parameters** option **> Monitoring** checkbox **> Enabled** flag is set to **true**.

Figure 193: KPI Monitoring Enabled flag



You can modify the **Default event expiration time** of 10080 minutes = 7 days. It is recommended to *not* change the **KPI deviation percentage** (dev% default = **20**) unless asked to do so by Technical Support. Deviation for regular monitors is calculated as follows:

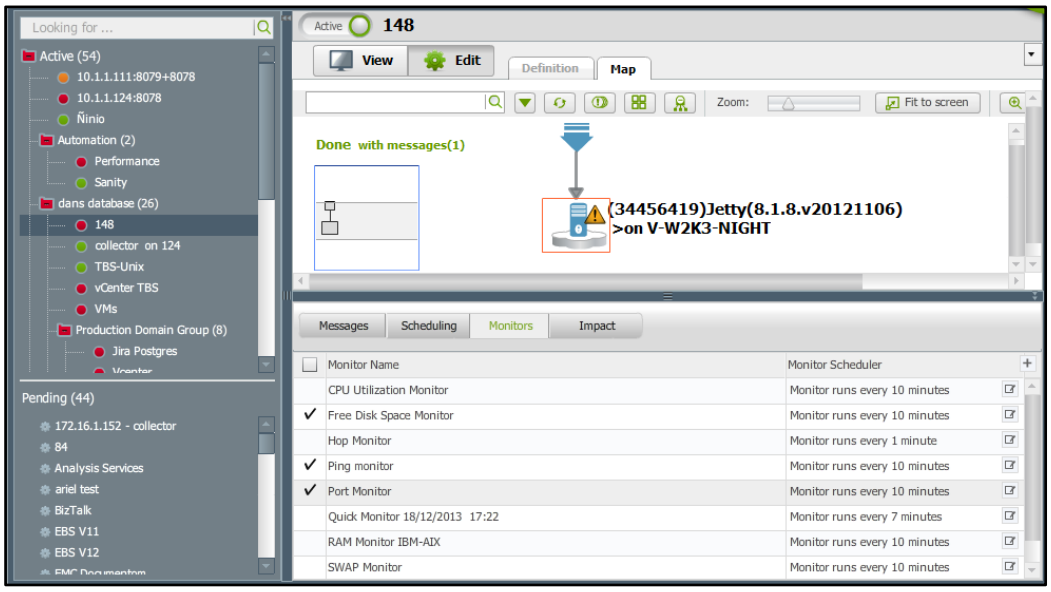
For ascending thresholds, deviation value = value that is dev% below the lowest threshold.

For descending thresholds, deviation value = value that is dev% below the highest threshold.

KPI = 100 * Abs (last value – the deviation value) / the deviation value.

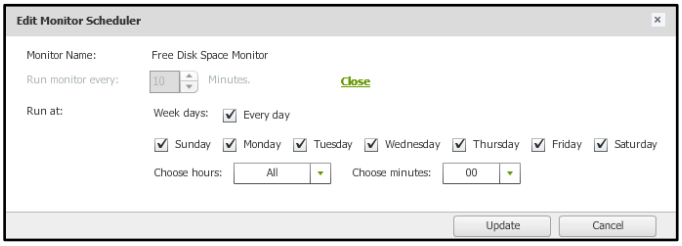
Display the relevant business service topology Map in **Edit** mode. Select the CI whose performance is to be monitored. Click the **Monitors** tab and ensure that the checkboxes for the desired monitors are selected in the **Monitors** panel. You can select the **Monitor Name** checkbox to toggle all of the listed monitors on or off or you can select or clear individual monitor checkboxes on the left side.

Figure 194: Business Service Topology Map in Edit mode



To modify a **Monitor Scheduler**, click that monitor's small checkbox in the column on the right side. The **Edit Monitor Scheduler** dialog box is displayed.

Figure 195: Edit Monitor Scheduler dialog box

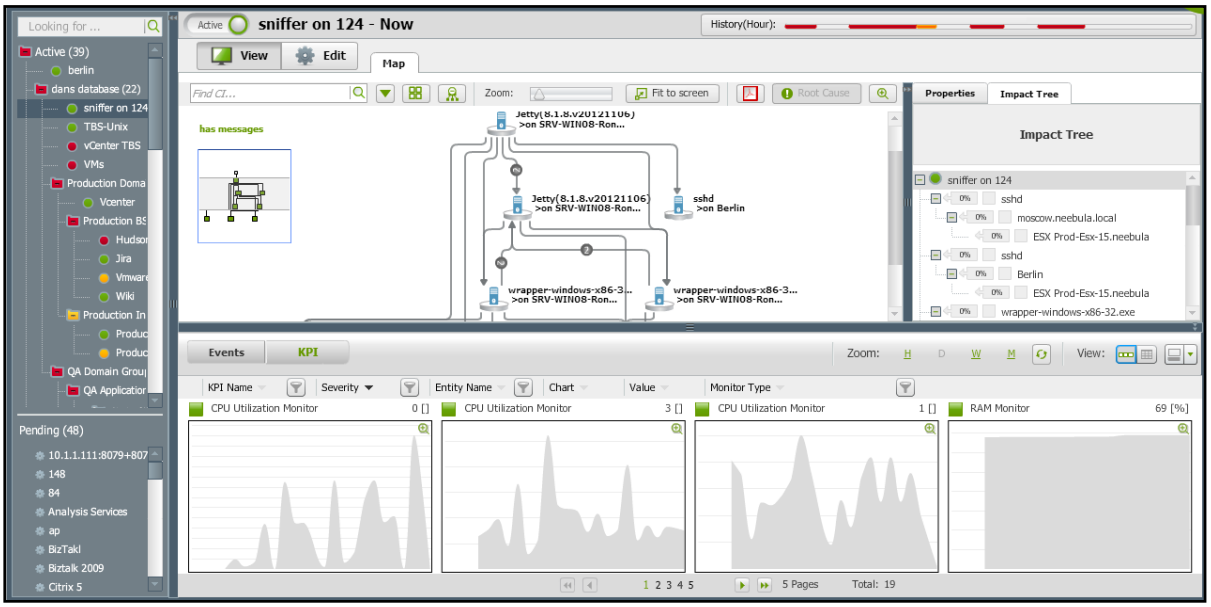


Use the up or down arrow to change the frequency (in minutes) *or* click **Advanced scheduling** to display the **Edit Monitor Scheduler**. Specify the days and time when the monitor should run, click Update to save the changes or Cancel to not save them and click the **Close** link.

Displaying KPIs

Select a CI, a Business Service, a Group, a node that contains groups, or even the **Active** root in the top left pane and click the KPI button to display a table or thumbnail graphs of KPIs in the bottom pane for the monitors that have been defined and whose checkboxes have been selected.

Figure 196: Displaying KPI thumbnails of the first 4 of 19 monitors



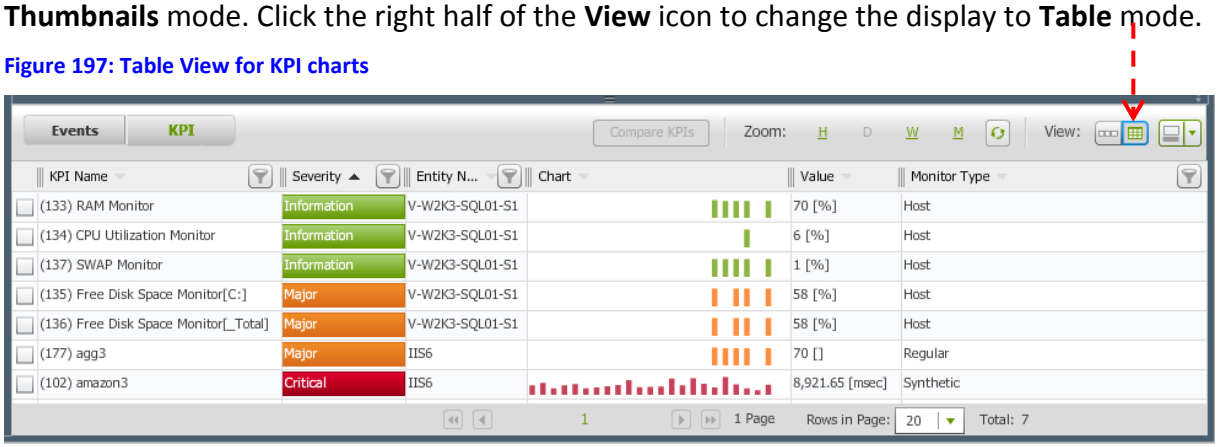
Infrastructure vs. Business Service Perspective

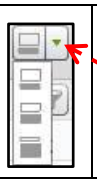
KPI data can be collected from an infrastructure (system architecture) perspective or a business service perspective. To toggle the KPI data collection perspective, click the **User perspective view** icon near the top of the **Monitoring** screen.

Table View vs. Thumbnails View

KPI information can be displayed in **Table** view or **Thumbnail** view. The default View is the last View that was used. Click the left half of the **View** icon to change the display to **Thumbnails** mode. Click the right half of the **View** icon to change the display to **Table** mode.

Figure 197: Table View for KPI charts





To change the vertical space allocated for KPI tables or thumbnail graphs, click the down arrow next to the right edge of the bottom pane and select the top (smallest), middle, or bottom (largest) area option.

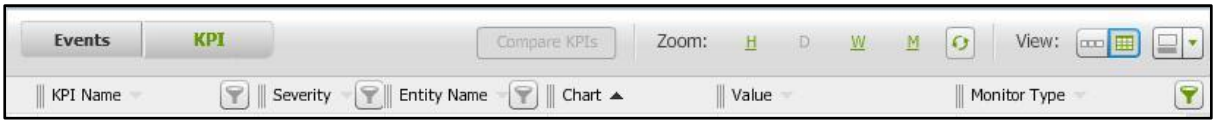
KPIs can be viewed for various periods of time. In the **Zoom** area, click **H**, **D**, **W** or **M** to display the tabular or graphical data for a period of time whose length is an hour, day, week or month. Data is cumulated for the week and month displays

To display a monitor's graph in the upper pane, select its checkbox near the left margin and click View KPI. To compare the graphs of two, three or four (but not more) monitors in the upper pane, select their checkboxes and click Compare KPIs.

KPI Filters

The same filters are available in both **Thumbnails** view and **Table** view.

Figure 198: KPI filters



When a filter is being used, its button is **green**. When it is not being used, its button is **grey**.

KPI Name Filter

When you click the **KPI Name** filter button, its filter criteria box is displayed. If this filter is being used, monitors whose name does not contain one of the specified text strings are not displayed.

Figure 199: KPI Name filter

To specify a text string, type the string in the **KPI Name** text box and, while the cursor is still in the text box, press the **Enter** key. Each specified string is displayed with its checkbox selected in a push-down stack. After the first string is specified, the **Select All**, **Unselect All** and **Clear All** commands can be used. Click the **x** in the top right corner to close the criteria box and apply the filter.

Severity Filter

The **Severity** filter prevents the display of monitors whose severity level is less than the position of the filter's slide. Select the slide position, then click the **x** to close the slide and apply the filter.

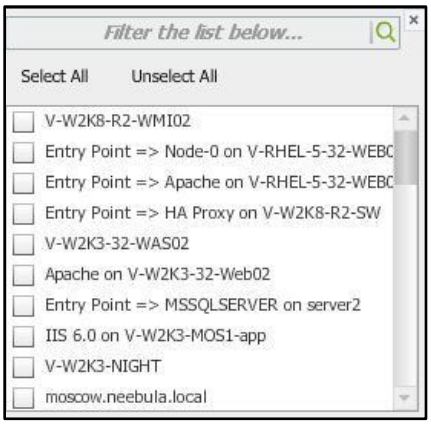
Figure 200: KPI Severity filter

The system-wide default status of the slide is the last location that was set. If the slide is in its leftmost position, the Severity filter button is **grey**. Otherwise it is **green**.

Entity Name Filter

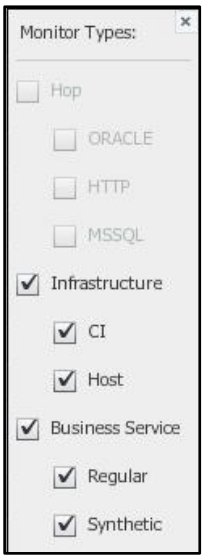
When you click the **Entity Name** filter button, its criteria box is displayed.

Figure 201: KPI Entity Name filter



This box contains the names of all entities whose monitors are relevant. Click **Select All** or select the checkbox of each entity whose monitors should be displayed. Click **Unselect All** to clear all of the checkboxes. Click the **x** in the top right corner to close the criteria box and apply the filter.

Monitor Types Filter



When you click the **Monitor Type** filter button, the Monitor Types criteria box is displayed. By default, all of the **Infrastructure** and **Business Service** monitor types are selected. You can uncheck any of the selected checkboxes to exclude that monitor type from the KPI display. If no checkbox is selected, all of the monitor types are displayed. Click the **x** in the top right corner to close the criteria box and apply the filter.

Sorting the KPI columns

Place the cursor over the name in the header of the column you want to sort. After the cursor changes to a hand, left-click to sort that column in ascending order. Click the same header name again to reverse the sort order. When sorting on any column other than **KPI Name**, the secondary sort order is **KPI Name** in ascending order.

A **Chart** column sort causes the data to be sorted by the number of observations (measurements) that were obtained during the relevant time interval. When the **Chart** column is sorted in descending order, entities whose monitor was not operational for all or part of the relevant time interval will be at or near the bottom of the list.

Displaying KPI detail in the Upper Panel

You can drag up to 4 thumbnail graphs into the **Map** or **Dashboard** upper area to view them in detail.

Figure 202: KPI display after dragging 4 CPU Utilization Monitors into the topology Map area

The **H D W M** (Hour, Day, Week, Month) Zoom mechanisms in the upper and lower panels work automatically and independently. Changing either one does not affect the other. However, when using the

mechanism to change the date-time range, the change is not implemented until you click the  Update KPI button.

If the cursor is placed on a KPI graph line in the upper area of the screen, a tool tip displays the KPI name, its date and time, and its 'value'. In the image below, 3 CPU monitors are compared.

Figure 203: Comparing the KPI graphs of 3 CPU monitors

To delete the 2nd, 3rd and/or 4th KPI chart from the upper area, click the **x** at the right edge of its label at the bottom of the graphic display.

The first KPI chart displayed in the upper area *cannot* be deleted in this manner.

You can delete all KPI charts from the upper area by clicking the **Map** tab or **View** button

(see Figure 202) to display the regular topology Map or by clicking 

in the upper left corner to display the Dashboard.

Chapter 9: Viewing Business Service History

This chapter contains the following topics:

Concepts

To help you troubleshoot when, how, and why a business service developed a problem, ServiceWatch enables you to view the business service's history. When the topology **Map** is displayed in 

mode, the **History** feature enables you to:

- See when changes to the topology of the business service (and related business services) occurred, and to view a description of those changes.
- View the topology of the business service (or related business services) as it was at a selected point in time (for example, immediately after a particular topology change).
- Select two points in time and generate a topology map that indicates objects that were added, deleted, and changed, as well as objects that remained the same.
- Compare changes made in related business services. This can help determine when and how a problem began.

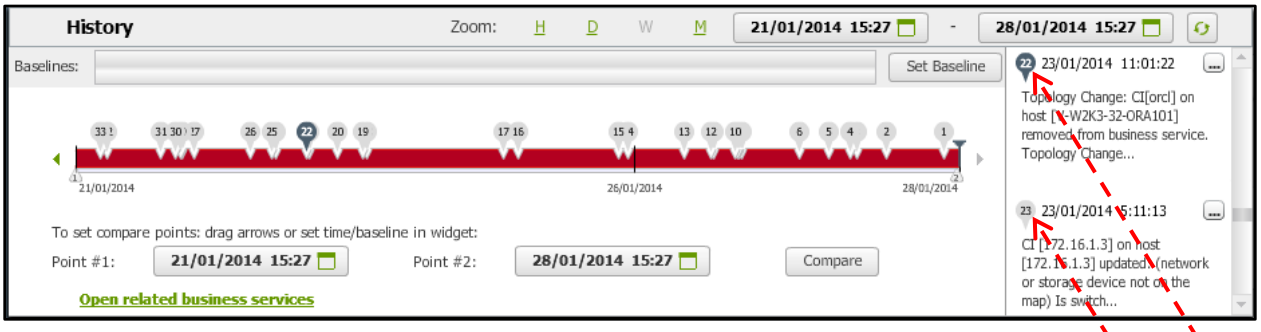
Viewing a Business Service's History

1. If the topology **Map** for the desired business service is not already displayed, double-click its tile or bubble in the Dashboard or click that business service in the **Active** tree, then click 

.
2. Click the **History** preview strip 

to display the **History** panel (Figure 204) for this business service.

Figure 204: History panel for the previous week



The previous week's history is displayed In Figure 204. Two labeled events (and) are described in the pane on the right side of the **History** panel.

The default period of time displayed is the period that was displayed the last time this feature was used. You can change the period of time displayed by clicking the letter **H**, **D**, **W** or **M** after the word **Zoom**.

- H displays the past hour (the previous 60 minutes)
- D displays the past day (the previous 24 hours)
- W displays the past week (the previous 168 hours)
- M shows the period since the same time of day on the same day of the previous month

The time line in the **History** panel contains 3 slides, two up-arrow slides on the bottom and one down-arrow slide on the top. The default positions of the two up-arrow slides are at the beginning (left edge) and end (right edge) of the time line. You can move these slides to any desired position on the timeline to specify the exact beginning and end of the time period for the **Compare** feature.

The default position of the down-arrow slide above the timeline is 'now' at the right edge of the time line. You can move this slide by dragging its vertical line to any point within the timeline. The topology **Map** will then be displayed as of that point in time.

Clicking the 

button in the **History** pane displays data about each modification to the topology that was made within the period defined by the timeline up-arrows.

Notes about the timeline:

- You can select and change the scale (hours, days, weeks, months).
- Above the timeline, numbered call-out circles indicate when topology changes occurred.
- The color of the timeline is the color of business service status at that time (except green is shown as white during time intervals when there was no problem).
- The numbered call-out circles enable you to display topology and perform comparisons as of specific times (as discussed in this chapter).
- Numbered call-out circles are **green** for CI removal and attribute changes that occur during a scheduled change interval. However, Topology changes are displayed in the usual way.

3. Perform any of the following actions, as needed:

Table 10: Business Service History actions

Action	Instructions
To change the scale of the timeline	In the **Zoom** area above the timeline, click the appropriate time interval (**H** = Hour, **D** = Day, **W** = Week, **M** = Month).
To display details of a numbered topology change in a tooltip	Let the cursor hover over the call-out circle, for example  , or  , whose number is that of the change to display.
To display topology as it was immediately after a numbered topology change	Click the timeline under the numbered call-out circle or drag the down-arrow to that location. The down-arrow is repositioned and the topology is displayed as of that time. The selected time is displayed in the title bar of the **Map**.
To display topology as of the current time	Click the Show Now link above the timeline.
To display: ▪ timelines for related business services ▪ a description of all topology changes ▪ the same topology at 2 different times	See DISPLAYING AND COMPARING TOPOLOGY CHANGES AND DETAILS
If the arrow at the left  or right  end of the time line is **green**, you can shift the time interval left (earlier) or right (later).	Let the cursor hover over the green arrow until it becomes a hand, then click once for each shift: 10 minutes per hour, 3 hours per day, 1 day per week, or 1 week per month.

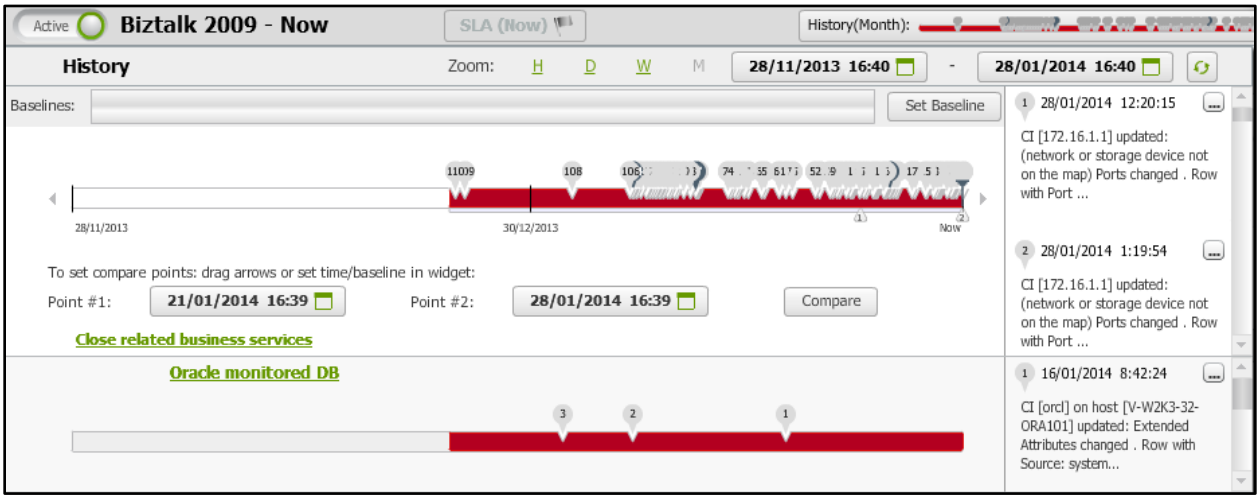
Displaying and Comparing Topology Changes and Details

The **History** panel contains an **Open related business services** link in the bottom left corner. If this link is not grayed-out, it displays a **History** pane (FIGURE 205) with the timeline of the selected topology plus the timelines of all related business services. Like the timeline in the regular **History** panel, these related business service timelines also contain markers indicating when changes occurred to the topology and details of each topology change (corresponding to the change markers) for each timeline.

You can compare and display how a business service topology looked and changed between two points in time by clicking the 

button.

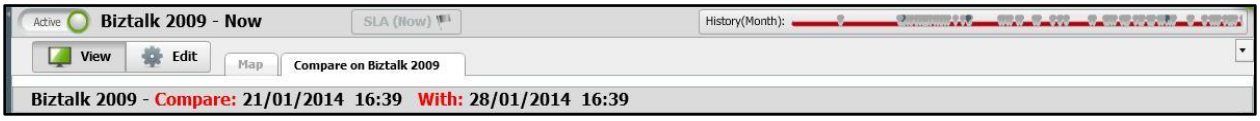
Figure 205: History pane with timelines for related business services



1. The area on the right side of the screen provides a numbered description of the topology changes that are indicated by each numbered change marker on the timelines.
2. As in the regular **History** panel, you can set the timeline scale to Hour, Day, Week, or Month.
3. To compare changes that occurred in the primary business service and one or more related business services between two points in time, do the following in the primary business service timeline:
   a. Move the up-arrow under the primary time line on the left to the earlier time point
   b. Move the up-arrow under the primary time line on the right to the later time point
   c. Click 

4. A **Compare on <business service name>** pane displays the topology of the primary and related business service. The top of that pane is similar to Figure 206.

Figure 206: History Compare on <business service name> pane (top only, topology *not* shown)



Notes:

- The **Compare from … To** header indicates the time range that is being compared.
- **Deleted** components have a dotted connection line and a **red** label.
- **Added** components have a dotted connection line and a **green** label.
- **Updated** components are indicated in **purple**.
  a. To view the properties of a related business service, display that business service in the topology Map. Changes to that business service's properties are indicated under Business Service Properties in the Properties panel.

Note: You can perform multiple comparisons with each related business service. Each comparison will appear in its own Compare on <business service name> panel.

b. To close a Compare on <business service name> topology panel, move the cursor to its tab and click its small close button  when it is displayed.

c. To close the Compare History panel, click the Close related business services link.

Chapter 10: Monitoring Networks

This chapter contains the following topics:

Concepts

The ultimate purpose of ServiceWatch is to detect problematic events that impact business services so that you can correct problems and maintain the health of the entire system.

Previous chapters focused on discovering the flow between applications and their host machines. But monitoring business services also requires monitoring the network connections between application hosts and identifying problems that involve network devices and ports.

When ServiceWatch performs discovery, it first discovers application flow connections. After it discovers an application flow connection, it discovers the network path between the applications. The network path consists of the application hosts at each end of the path, relevant network devices (switches, routers, etc.), ports and network cards along that path.

Network paths are displayed in a **Network Path** panel that is opened by right-clicking a path in a topology **Map**. The display in the **Network Path** panel is similar to the topology **Map** and uses color coding to flag problematic statuses.

Although you can manually modify topology in the topology **Map**, you cannot modify the path in the **Network Path** panel. However, parameters that you define elsewhere do affect the network path (see DEFINING SERVICEWATCH NETWORK PARAMETERS below).

Defining ServiceWatch Network Parameters

Network parameters as usually defined while performing other tasks. Be sure that you have performed the following tasks that involve network parameters:

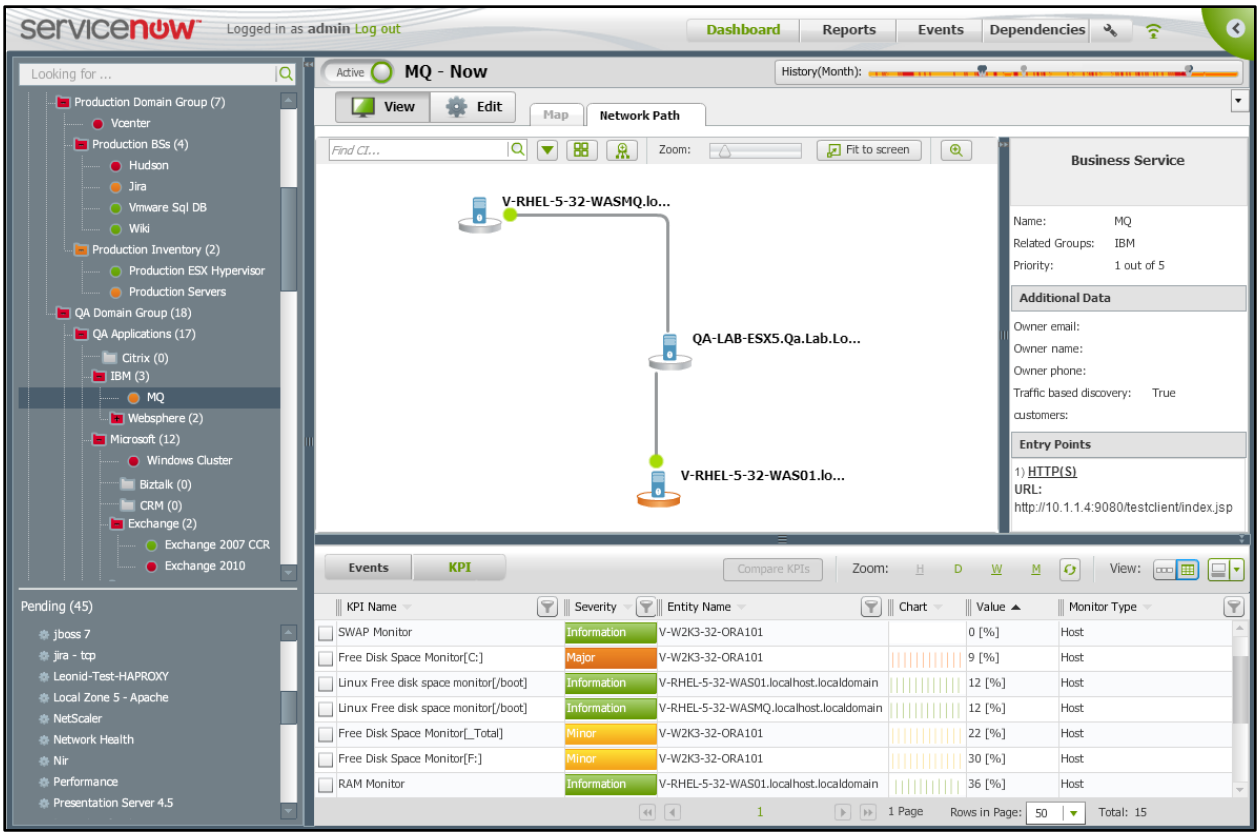
- Defining Network Discovery parameters (see Figure 111 on page 128). This enables ServiceWatch to discover network paths for application flow connections.
- Defining Network Device Impacts and Network impact statuses (see Defining the Impact of an Object on its Parent or Business Service). This enables ServiceWatch to determine the impact of network devices and ports on the business service.
- Binding Unsupported Network Events (see Define the Binding Rule for an Event). When an unsupported event is a network event, follow these instructions to select the CI type in the Binding Rule Definition screen:
  - ✓ To bind an event to an entire device (switch, router), select **host** as the CI type.
  - ✓ If the event should be bound to a port, select **host.port** as the CI type.

Displaying Network Path Details

1. Display the topology **Map** for the business service by clicking the business service in the **Active** tree or double-clicking its tile or bubble in the Dashboard **Monitoring** screen.
2. To display a path between two objects, right-click their connection and select **Show network path** in the pop-up menu. The **Network Path** panel is displayed (Figure 207).

Note: This step can be performed in **View** or **Edit** mode. The pop-up menus for these modes are different but both contain the **Show network path** option.

Figure 207: Network Path panel

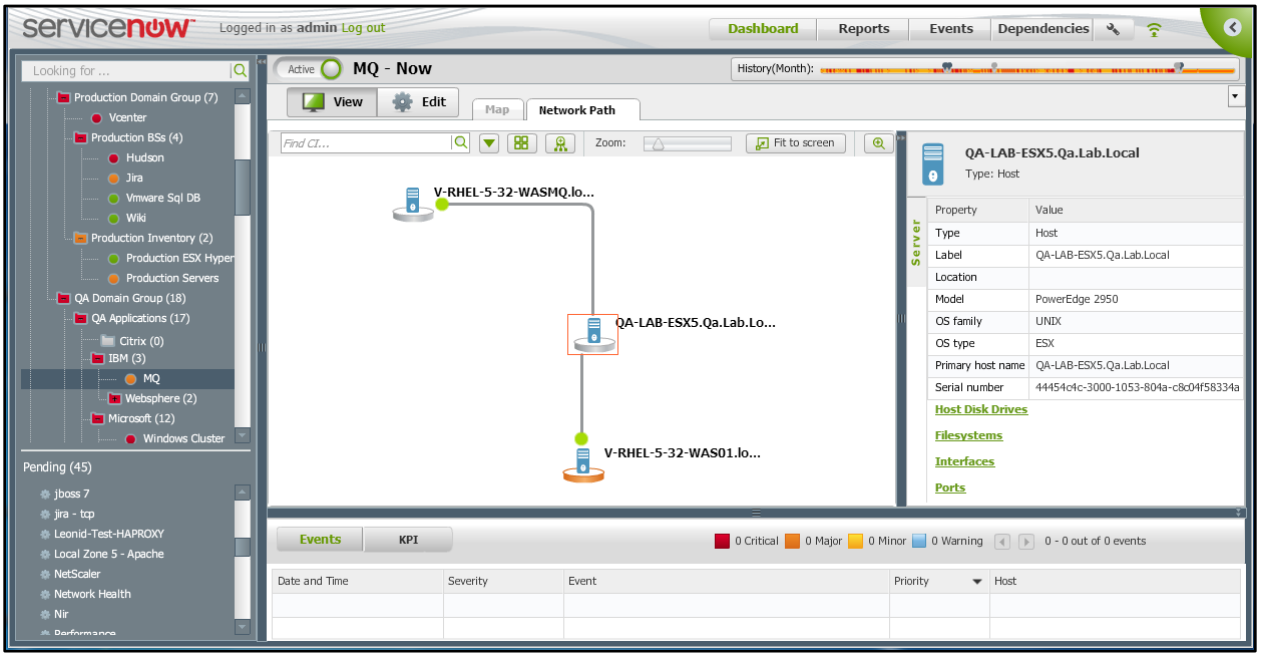


- ✓ Each circle at the end of a connection represents a port or entry point to a network device.
- ✓ Navigation aids in this panel (Find CI search box, Additional options down arrow, Host view icon, Overview icon, Zoom slide, Fit to screen button, and magnifying glass icon) work like topology Map navigation aids. See Table 8 on page 162.

Viewing Properties of a Connection

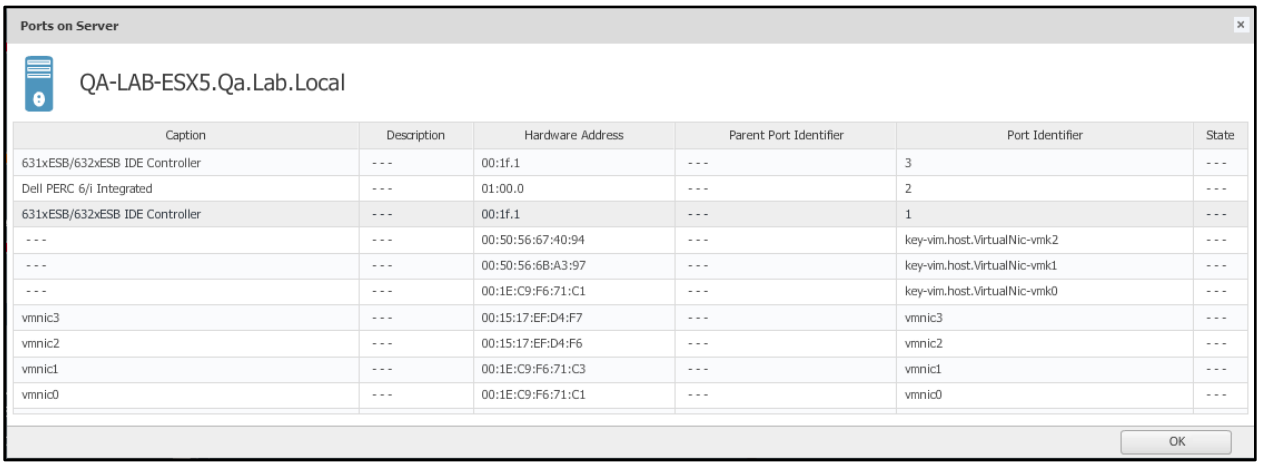
1. To display properties of an object in a network path, click the object's icon. The icon becomes surrounded by a red box and its properties are displayed in the right pane (Figure 208).

Figure 208: General Properties of an object in the Network Path



2. You can display data pointed to by an underlined link. For example, if you click **Ports** in Figure 208, a pop-up displays a table of port data (Figure 209). Click OK to exit the pop-up.

Figure 209: Ports screen – Properties table pop-up

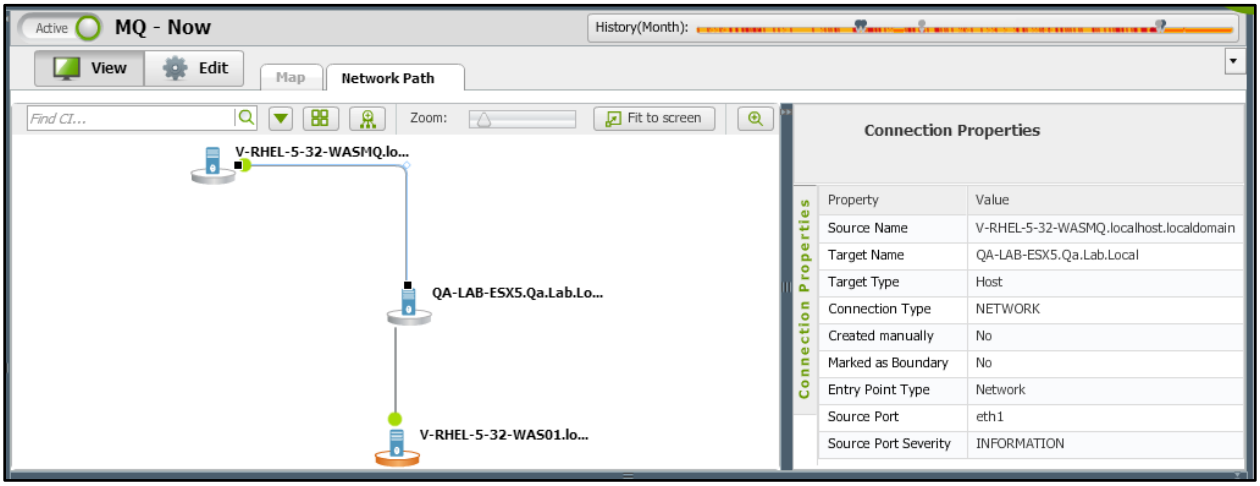


Notes:

- Connections between network devices in the path are indicated by solid gray lines.
- The color of the circle at the end of a connection indicates port or network card status.
- Dotted connection lines indicate there might be additional network devices that ServiceWatch could not discover. In this case, you should consider adding seed IPs or hosts (for instructions, see the text under Figure 111).
- Objects with a problematic status appear with color coding. Example: 

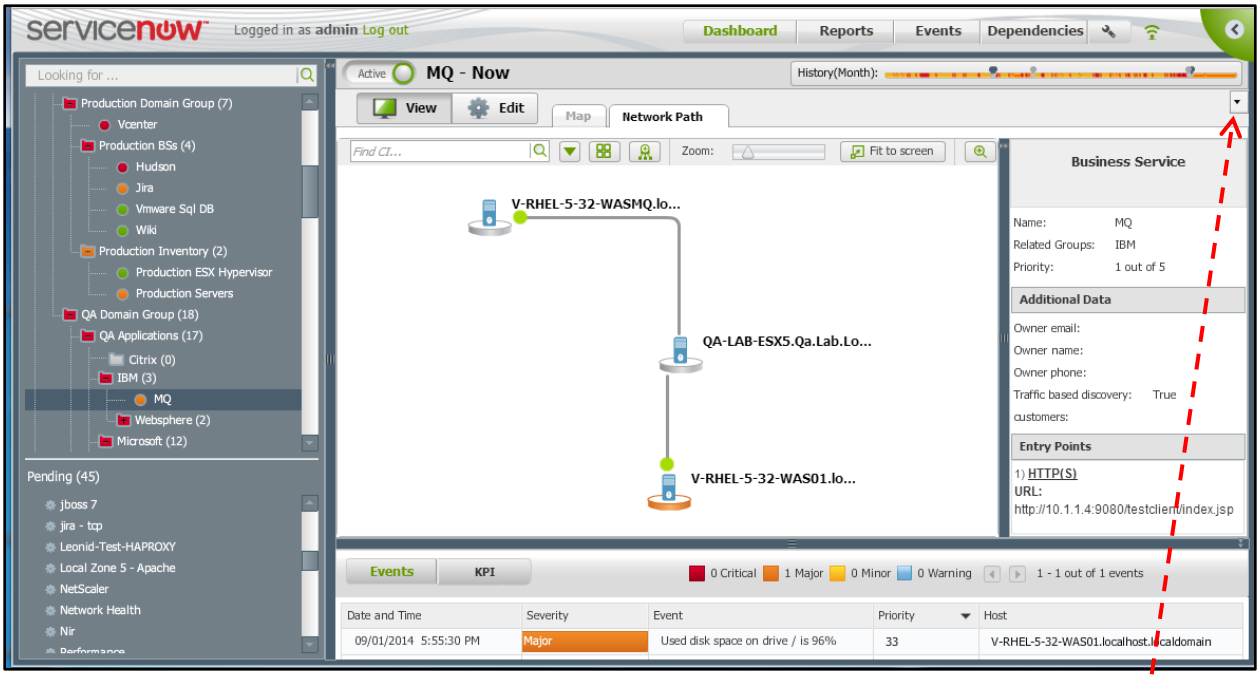
3. To display connection properties (including source and target port names) between two objects in the network path, click the connection between the objects. Two small black squares indicate the endpoints of the selected connection and its data is displayed in the Connection Properties area in the right pane of the Network Path panel (Figure 210).

Figure 210: Connection Properties – Network Path

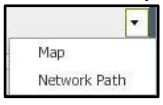


4. When you finish viewing the **Connection Properties** for a path, click anywhere in the **Network Path** topology panel. The properties of the business service will be displayed in the area on the right side of the **Network Path** topology.

Figure 211: Business Service Properties in Network Path panel



5. To close the **Network Path** panel and return to its Topology **Map**, click the down-arrow near the top right corner and select **Map**.



Checking the Health of a Network Path

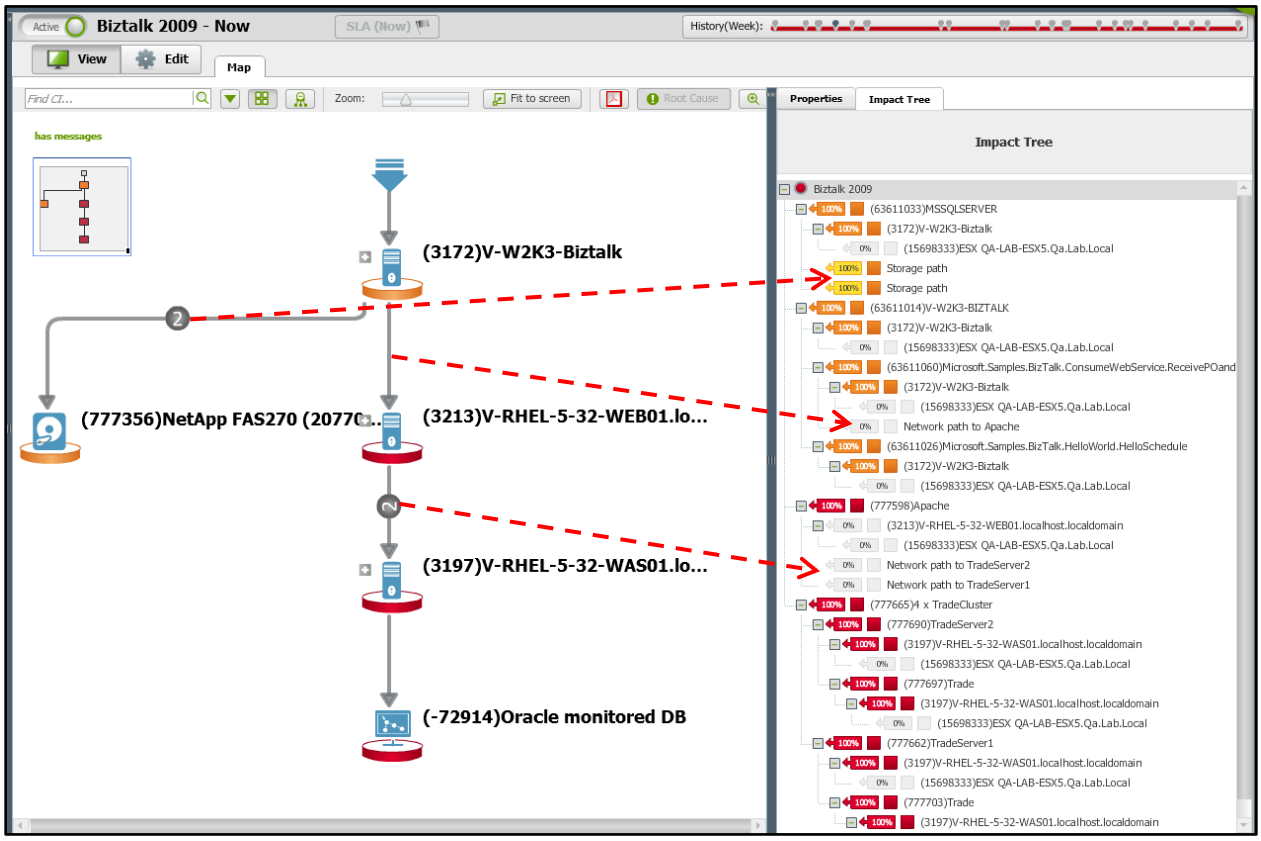
As described in Defining the Impact of an Object on its Parent or Business Service on page 143, the pane underneath the topology **Map** in **Edit** mode enables the impact status of components to be defined. Network path status is included in this process (see item 2 f on page 146).

You can view the health of a network path by displaying the business service **Impact Tree** panel in the pane on the right of the topology **Map** in **View** mode.

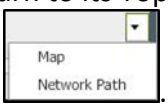
1. Click the business service you want to monitor in the **Active** tree, or double click the tile or bubble of that business service in the Dashboard. When the topology **Map** is displayed, click 

and click the **Impact Tree** tab in the pane on the right side. The red dashed lines point to the Storage and Network Path impact status data in the **Impact Tree** (Figure 212).

Figure 212: Network Status in the Impact Tree



2. To display a network path between two applications, right-click the connection between them in the topology **Map** and select **Show network path**. The **Network Path** pop-up menu opens.
3. To display general properties of an object in the network path, click the path. The properties are displayed in the right pane of the **Network Path** panel (Figure 210). Click a link to display a pop-up listing properties of the CI type identified by that link, e.g., **Interfaces** or **Ports** (Figure 209). Click **OK** to exit this pop-up.

4. When you finish viewing the **Connection Properties** for a particular path, click anywhere in the **Network Path** topology panel. The **Business Service Properties** will be displayed in the right pane of the **Network Path** panel (Figure 211).
5. To close the **Network Path** panel and return to its Topology **Map**, click the down-arrow near the top right corner and select **Map** 

.

Chapter 11: Storage Paths

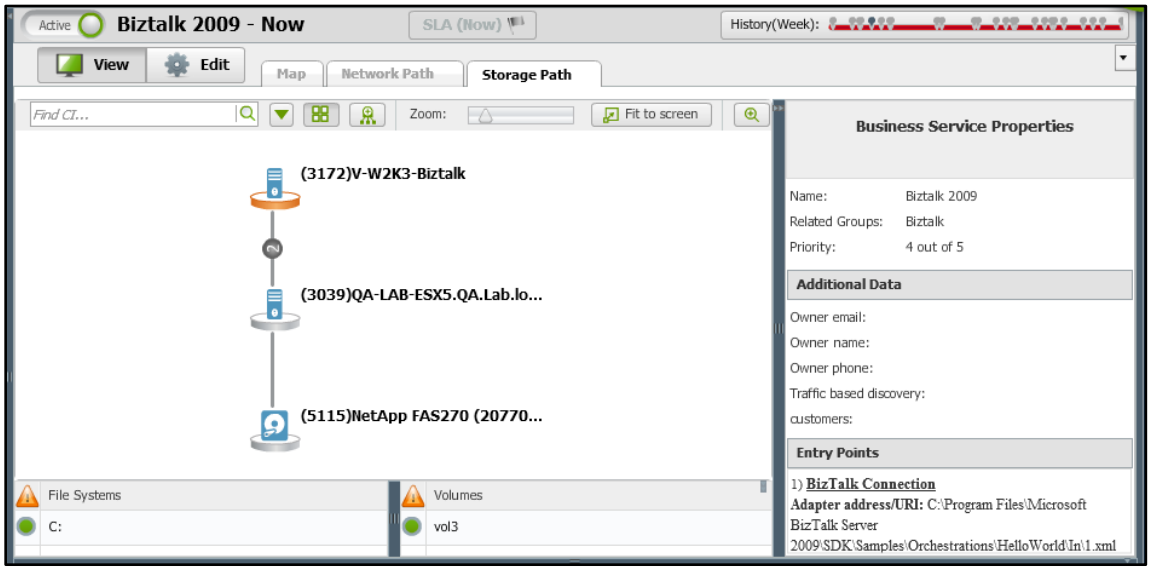
When storage devices are used, it is desirable to monitor the connections between the host and those devices. Storage devices and the paths to them can be discovered using Network Discovery. However, if a storage device for a business service has not yet been discovered, you can specify its IP address in the 

area at the bottom of the **Network Discovery** screen (Figure 111).

Storage paths are displayed in a **Storage Path** panel that is opened by right-clicking a storage path in a topology **Map** and selecting the **Show storage path** option. If there is more than one path, an option box enables you to select the desired path. For example:

The **Storage Path** panel is similar to the **Network Path** panel and uses color coding to flag statuses.

Figure 213: Storage Path panel in View mode



Although you can manually modify topology in the topology **Map**, you cannot modify the path in the **Storage Path** panel. However, parameters that you define elsewhere do affect the storage path.

Defining Storage Path Parameters

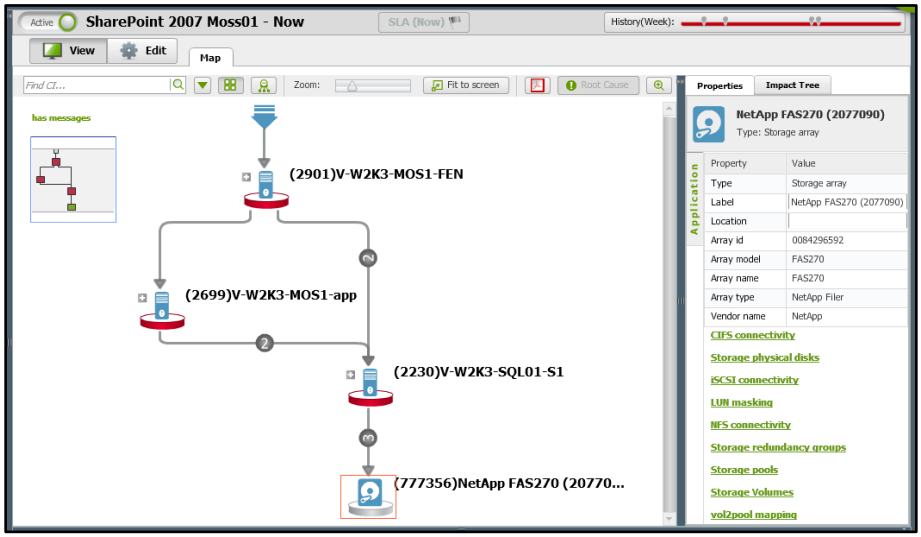
Storage path parameters have defaults, but you can define Network parameters and storage device impact rules when performing the following tasks:

- DEFINING SERVICEWATCH NETWORK PARAMETERS on page 206.
- Defining storage device impact rules so that ServiceWatch can determine the impact of storage devices on the business service.
  (See step 3g in DEFINING THE IMPACT OF AN OBJECT ON ITS PARENT OR BUSINESS SERVICE).

Displaying Storage Path Details

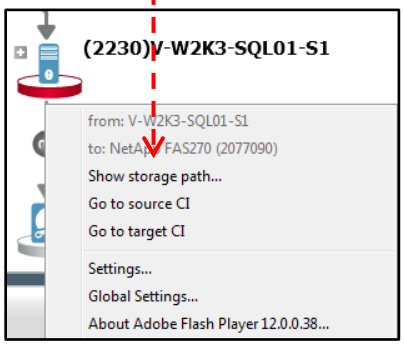
1. Display the topology **Map** for the business service that has a storage device by clicking it in the **Active** tree or double-clicking its tile or bubble in the Dashboard **Monitoring** screen.

Figure 214: Business Service topology with a Storage Array (NetApp FAS270)



2. To display a storage path between a host and storage devices, right-click the connection between them and select **Show storage path** in the pop-up menu.

Figure 215: Show storage path option in Connection right-click pop-up menu



Note: This step can be performed in **View** or **Edit** mode. The pop-up menus for these modes are different but both contain the **Show storage path** option.

If the connection represents more than one path, a path selection box is displayed.

Figure 216: Path selection box

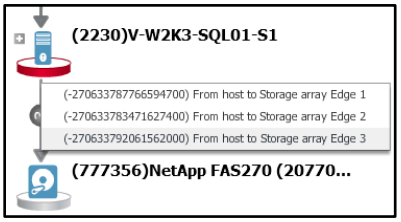
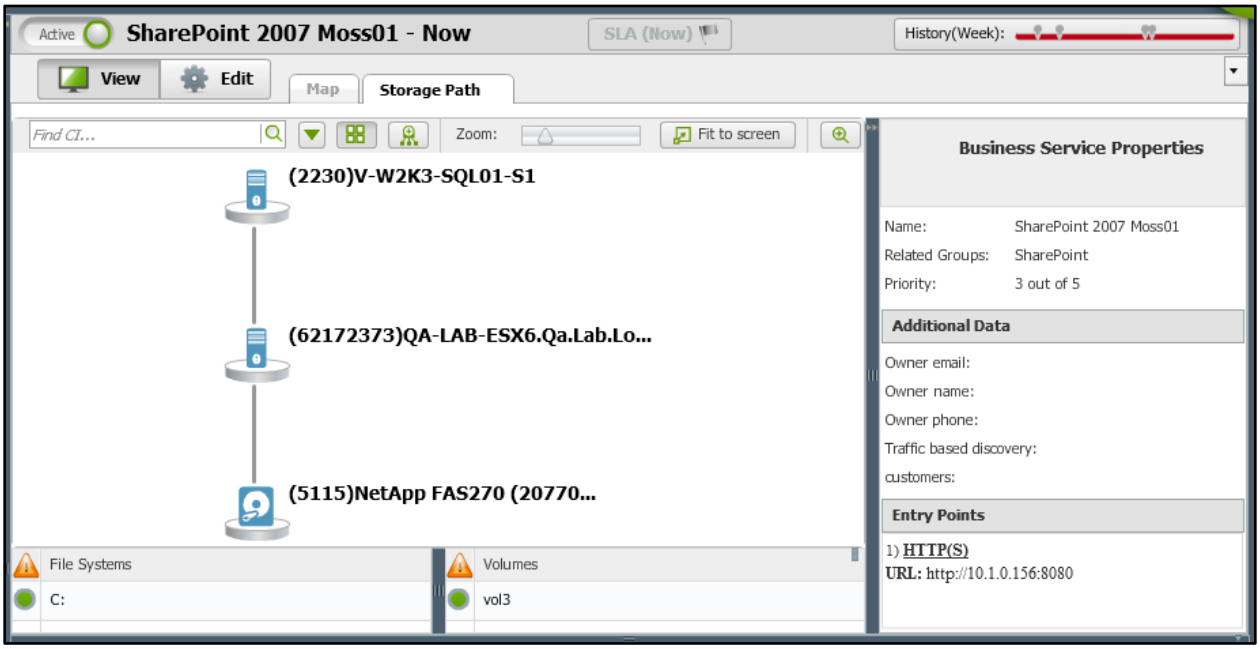


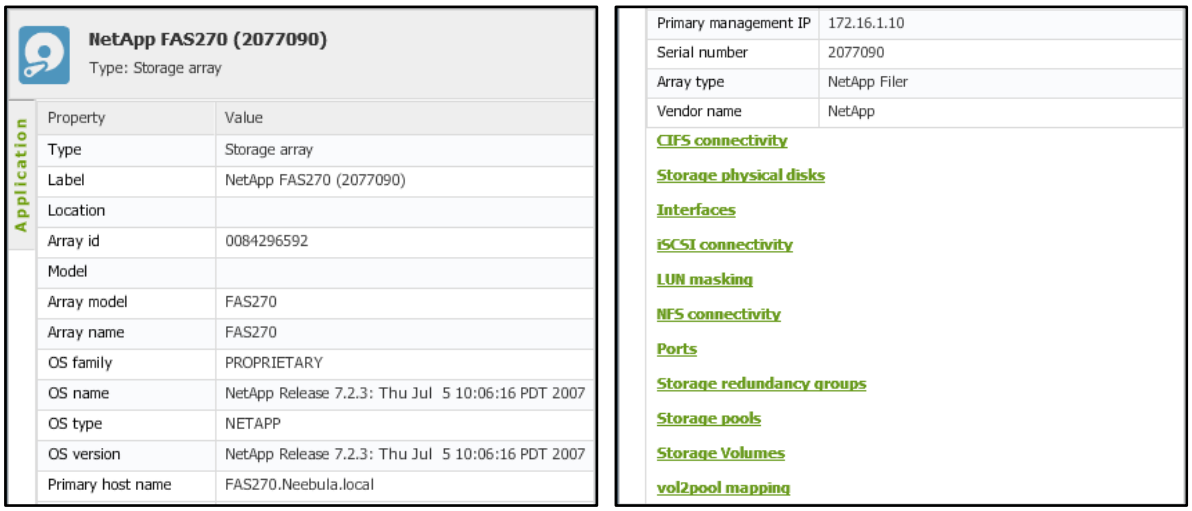
Figure 217: Storage Path panel

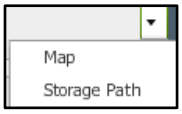


- ✓ Information about the File Systems on the Host and the Volumes on the storage device is displayed in the two panes under the **Storage Path** panel.
- ✓ Each circle at the end of a connection represents a port or entry point to the storage device.
- ✓ The Find CI search box, Additional options down-arrow, Host view & Overview icons, Zoom slide, Fit to screen button, and magnifying glass work like the topology Map navigation aids.

3. To display information about a network device in the storage path, click the device's icon. That icon becomes surrounded by a red box and data about the device is displayed in the right pane.

Figure 218: Storage device data displayed in right pane



4. To exit the **Storage Path** panel, click the **Map** tab, or the **Edit** or **View** button, or the down-arrow at the top right corner and select the **Map** option 

.

Chapter 12: Reports

Report Types

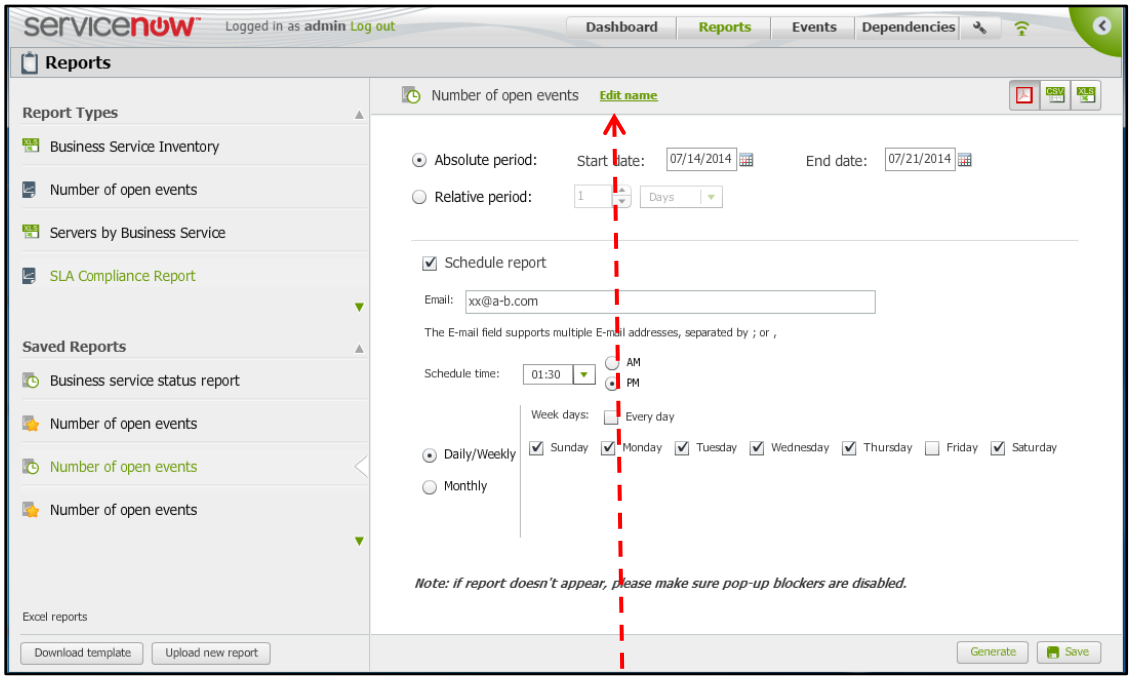
1. The following standard report types are currently available in ServiceWatch:
   - ✓ **Number of open events** for all nodes each day of the report period (Figure 224)
   - ✓ **SLA Compliance Report –** Indicates the extent to which Service Level Agreement requirements have been met. See Figure 225 on page 221.
   - ✓ **Servers by Business Service –** Lists all servers and the business services associated with each
   - ✓ **Business Service Inventory –** Lists all currently defined Business Services
   - ✓ **Business service status distribution report –** % time spent in each severity level (Information, Warning, Minor, Major, Critical) by each business service (Figure 228)
   - ✓ **Business service status report –** % uptime for each business service during the report period (Figure 226)
   - ✓ **Topology change report –** List of topology changes for the selected node(s) that occurred during the report period (Figure 227)
2. User-defined custom reports can be designed using the Excel Reports Generator on page 223.

Reports window

Click 

to display the Reports window (Figure 219) to define, schedule or generate a report. Select a Report Type to create a new report of that type or a Saved Report to be modified or generated.

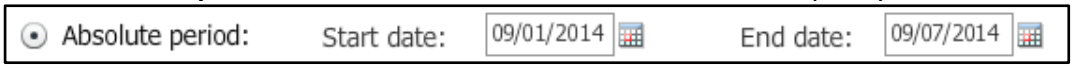
Figure 219: Reports window



3. To create a new report in one of the standard formats, select one of the **Report Types**.
4. To change the report name, click the **Edit name** link, modify the name and click **Finish**.
5. The format  buttons determine whether the report becomes a PDF, CSV or XLS file.

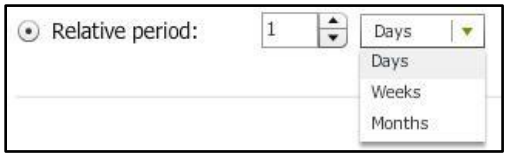
Report Time Period

6. Select the **Absolute period** radio button and use calendar icons to specify a **Start** & **End date**



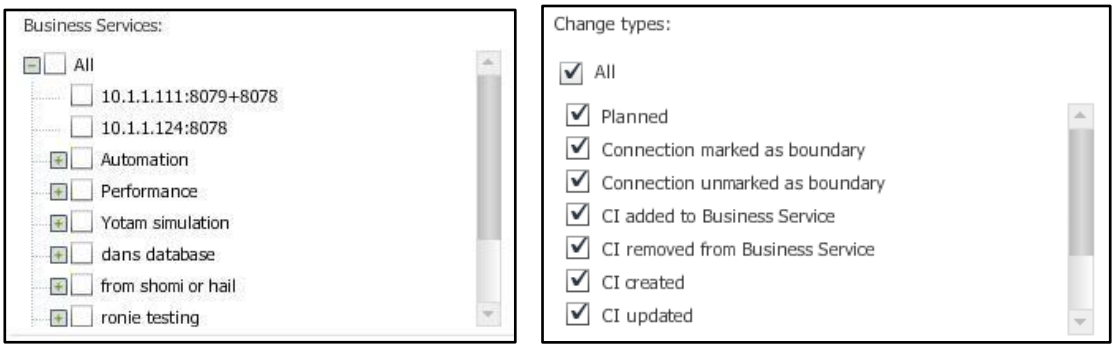
or

select the **Relative period** radio button and use the up and down arrows to specify a time interval from 1 through 1000 days, weeks or months (for example, 52 weeks) beginning 'now' during which the report will be generated.



7. If you are specifying a **Topology change report**, select the checkboxes of the **Business Services** and **Change types** that will be included in the report. For example:

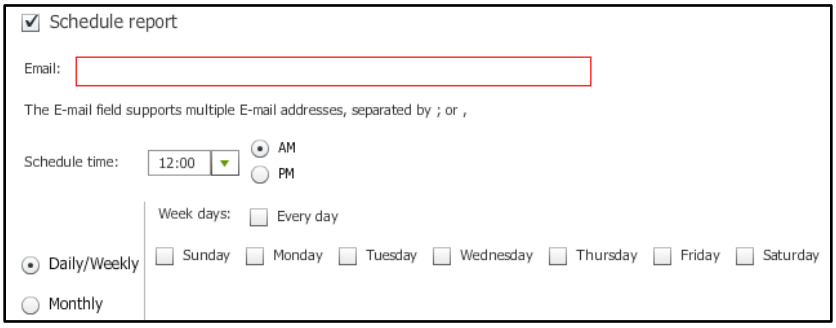
Figure 220: Checkboxes for Business Services and Change types



Schedule a Report

8. You can schedule a report at a specified time on one or more specific days of the week or on specific days of the month. Select the **Schedule report** checkbox. Specify an **Email** address to which the report will be sent, select a time in the **Schedule time** drop-down list, and check the desired days of the week or month …

Figure 221: Schedule report days-of-the-week settings



or the desired months and day of the month

Figure 222: Schedule report day-of-the-month settings

The clock icon  identifies scheduled reports that are generated automatically but can be generated manually at any time by the 

button. The star icon  identifies unscheduled reports that can only be generated manually.

9. To save a report so that it can be generated automatically or manually, click the 

button.

10. When the cursor hovers over the name of a **Saved Report**, information about that report is displayed in a tool tip and its delete icon [×] is displayed. To delete a report, click its [×] delete icon.

Figure 223: Saved Reports tool tip

11. To edit an existing report, click its row in the **Saved Reports** list and modify the appropriate parameters.

Sample Reports

Figure 224: Number of opened events report

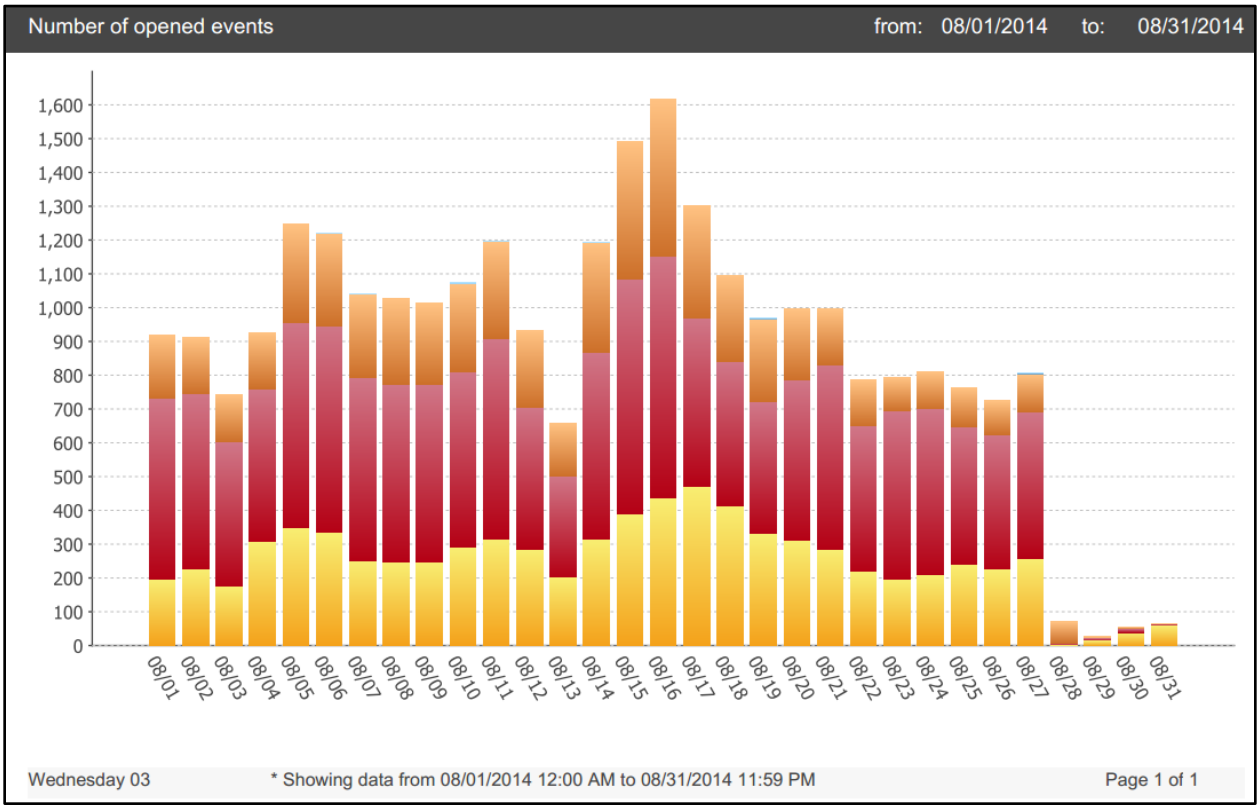
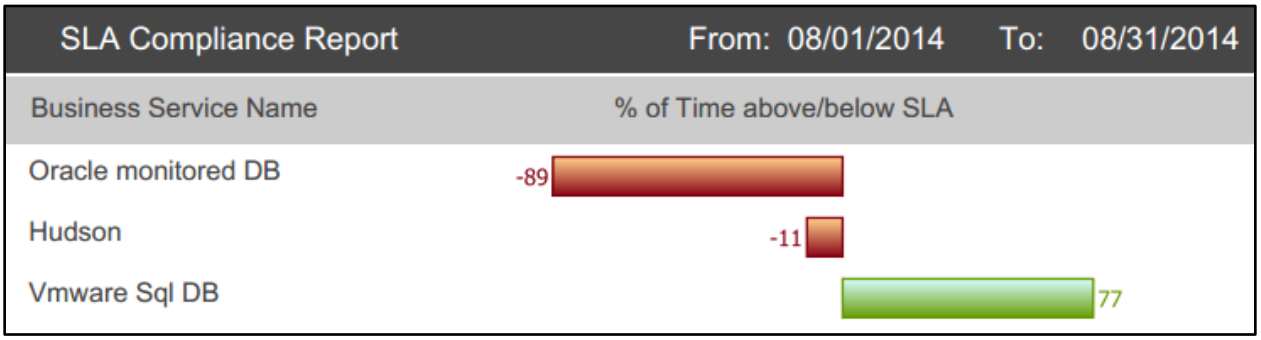
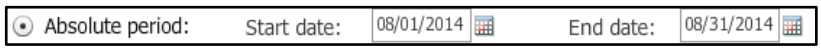


Figure 225: SLA Compliance Report



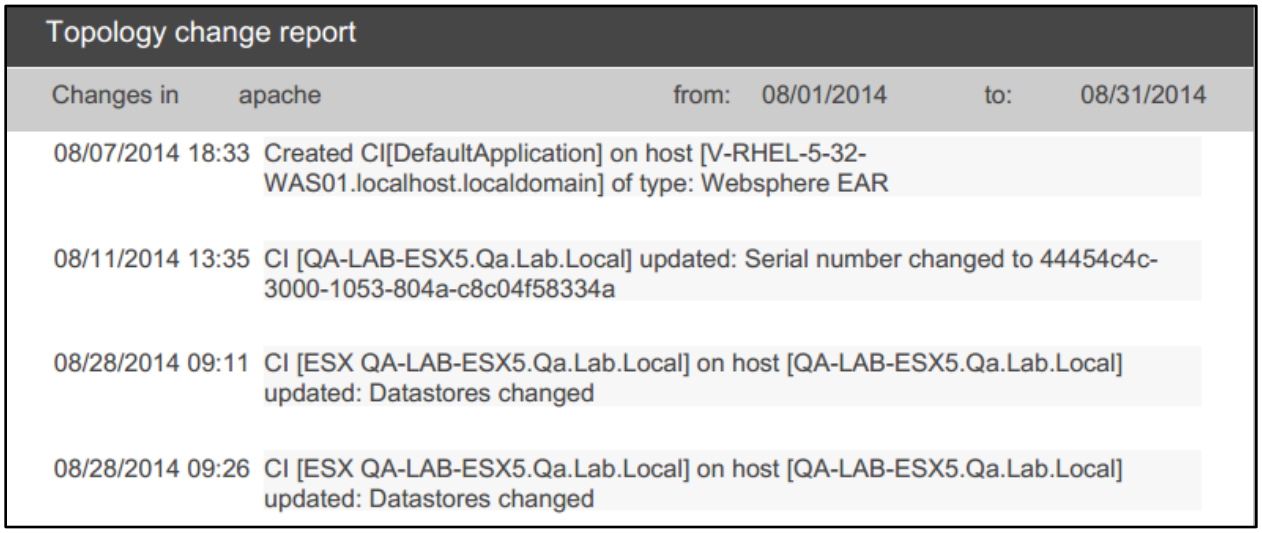
In the **SLA Compliance Report**, a **green** bar extending from the center to the right indicates the percentage by which a business service exceeds the level of service it is expected to provide. A **red** bar extending from the center to the left indicates the percentage by which a business service fails to reach its expected level of service.

The 

calendars define the date range of the data used in the SLA calculation. Or you can run the SLA report every *n* days/week/months.

Figure 226: Business service status report

Figure 227: Topology change report

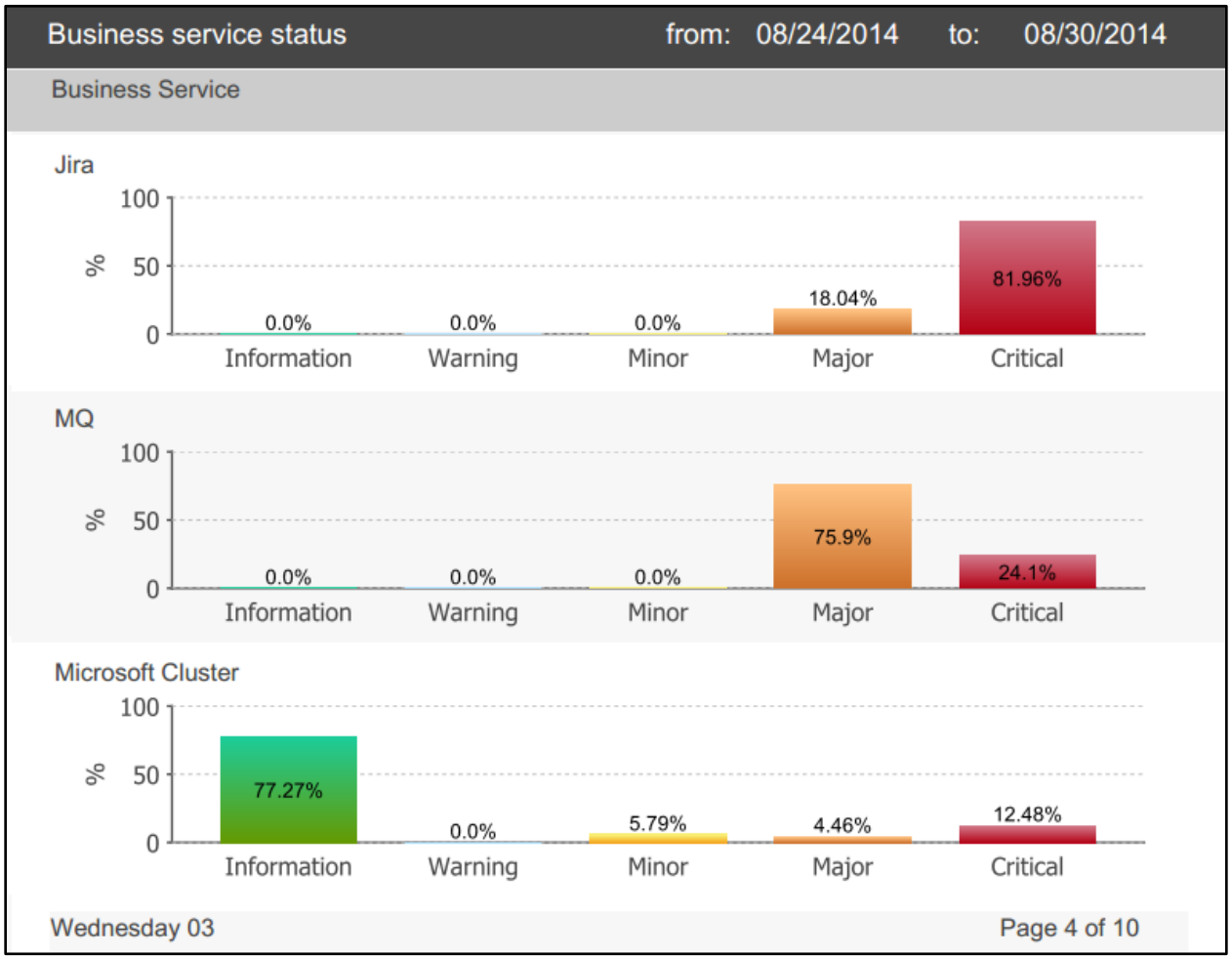


Topology change report

Changes in apache from: 08/01/2014 to: 08/31/2014

08/07/2014 18:33	Created CI[DefaultApplication] on host [V-RHEL-5-32-WAS01.localhost.localdomain] of type: Websphere EAR
08/11/2014 13:35	CI [QA-LAB-ESX5.Qa.Lab.Local] updated: Serial number changed to 44454c4c-3000-1053-804a-c8c04f58334a
08/28/2014 09:11	CI [ESX QA-LAB-ESX5.Qa.Lab.Local] on host [QA-LAB-ESX5.Qa.Lab.Local] updated: Datastores changed
08/28/2014 09:26	CI [ESX QA-LAB-ESX5.Qa.Lab.Local] on host [QA-LAB-ESX5.Qa.Lab.Local] updated: Datastores changed

Figure 228: Business Service Status Distribution report



Excel Reports Generator

This feature provides an Excel template for designing and generating custom made reports.
It requires Microsoft Office 2007 or later.

Note: When using Microsoft Office 2010 or later, Visual Basic should be enabled for all applications in order for the Excel Reports Generator to work properly.

When using the Excel Reports Generator, be sure that all of the following steps are or have been performed:

1. Download the Reports Generator template (see below)
2. Unzip the downloaded file
3. Run the appropriate 32 or 64-bit installer
4. Open Excel
5. Configure Excel Security (see below)
6. Configure the WMI collector to execute Excel-reports (see below)
7. Create the report query and the report
8. Upload the report template
9. Rename and schedule the report
10. If there are changes to the report, download, update and upload the report.

Download the Reports Generator

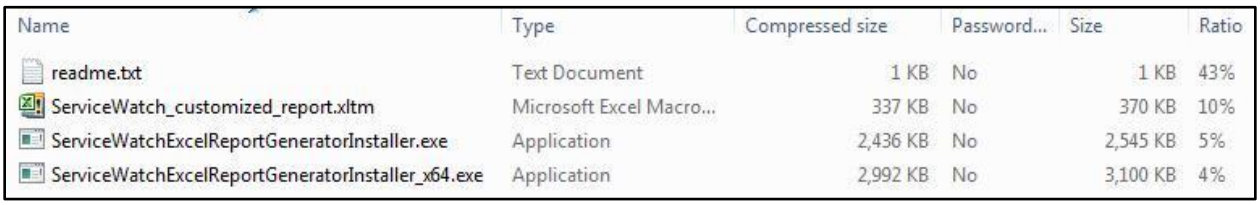
To download the zip file required for this feature, click the 

button at the bottom left corner of the **Reports** screen (Figure 219). This download needs to be performed only once on each ServiceWatch platform.

Your browser should enable you to save the downloaded zip file.

and extract and save these 4 files:

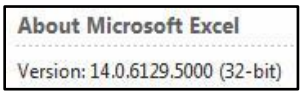
Figure 229: Four Excel Reports Generator files extracted from the zip file



Name	Type	Compressed size	Password...	Size	Ratio
readme.txt	Text Document	1 KB	No	1 KB	43%
ServiceWatch_customized_report.xltm	Microsoft Excel Macro...	337 KB	No	370 KB	10%
ServiceWatchExcelReportGeneratorInstaller.exe	Application	2,436 KB	No	2,545 KB	5%
ServiceWatchExcelReportGeneratorInstaller_x64.exe	Application	2,992 KB	No	3,100 KB	4%

Read the **readme.txt** file.

Open your Microsoft Office Excel application and click **File > Help** to determine whether your Excel application (*not* your Windows operating system) is 32 or 64-bit. You should see a description similar to:



For 32-bit Excel, run the extracted **ServiceWatchExcelReportGeneratorInstaller.exe** file.
For 64-bit Excel, run the extracted **ServiceWatchExcelReportGeneratorInstaller_x64.exe** file.

These exe files produce an **ActiveQueryBuilderXControls.ocx** file. The default location for saving this file is **C:\ServiceWatchQueryBuilder**. Select the location to store this file. The selected extraction path should contain the **ActiveQueryBuilderXControls.ocx** file.

Figure 230: Extraction path for the ServiceWatch Query Builder

File Extensions for Report Templates and Reports

Use the following file extensions when creating a report template and when updating an existing report.

- Downloaded template: `*.xltm`
- Uploaded template after editing: `*.xlsm`
- Downloaded and updated reports: `*.xlsx`

Configure Excel Security

First, install Excel 2007, 2010 or 2013 on the ServiceWatch server that runs the WMI collector and configure Excel to give administrator rights to a particular user name. Then configure that ServiceWatch server to use that user name when running the Excel report.

Excel 2007

Method 1

1. Open Excel.
2. If the Enable Macros dialog box is not displayed, select **Tools > Macro > Security** in the Excel Menu. A dialog box will open. In that dialog box, select **Medium Security** and click **OK**. Close Excel and re-open it. The **Enable Macros** dialog box should be displayed.
3. The **Enable Macros** dialog box should indicate the location of the file and contain the text: 'Macros contain viruses. It is always safe to disable macros, but if the macros are legitimate, you might lose some functionality'
4. There are 3 buttons below this text: **Disable Macros**, **Enable Macros** and **More Info**. Click **Enable Macros**.

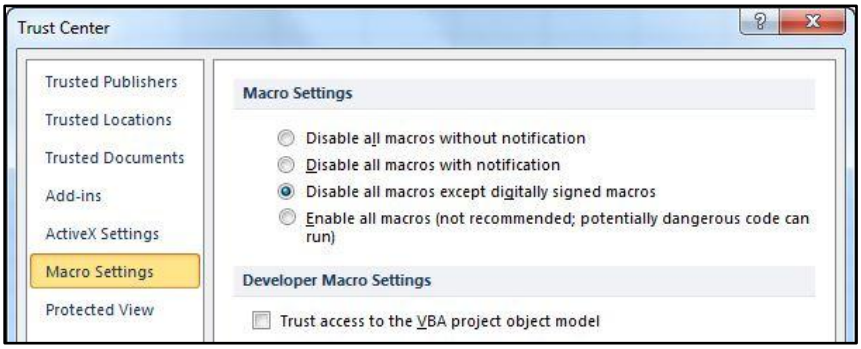
Method 2

1. If the Developer tab is not displayed, click the **Microsoft Office** Button, click **Excel Options**, and then in the **Popular** category, under **Top options for working with Excel**, click **Show Developer tab in the Ribbon**.
2. Click the **Developer** tab. In the **Code** group, click **Macro Security**.
3. In the **Macro Settings** category, under **Macro Settings**, click **Enable Macros**.

Note: Changes made in the **Macro Settings** category in Excel apply only to Excel and do not affect other Microsoft Office programs. You can also access the Trust Center via the **Excel Options** dialog box. Click the **Microsoft Office Button** and click **Excel Options**. In the **Trust Center** category, click **Trust Center Settings**, and then click the **Macro Settings** category you want.

Method 3

1. With an Excel file open, click the **Office** button.
2. Click **Excel Options** (at the bottom).
3. Select Trust Center > Trust Center Settings. The Trust Center dialog box is displayed.

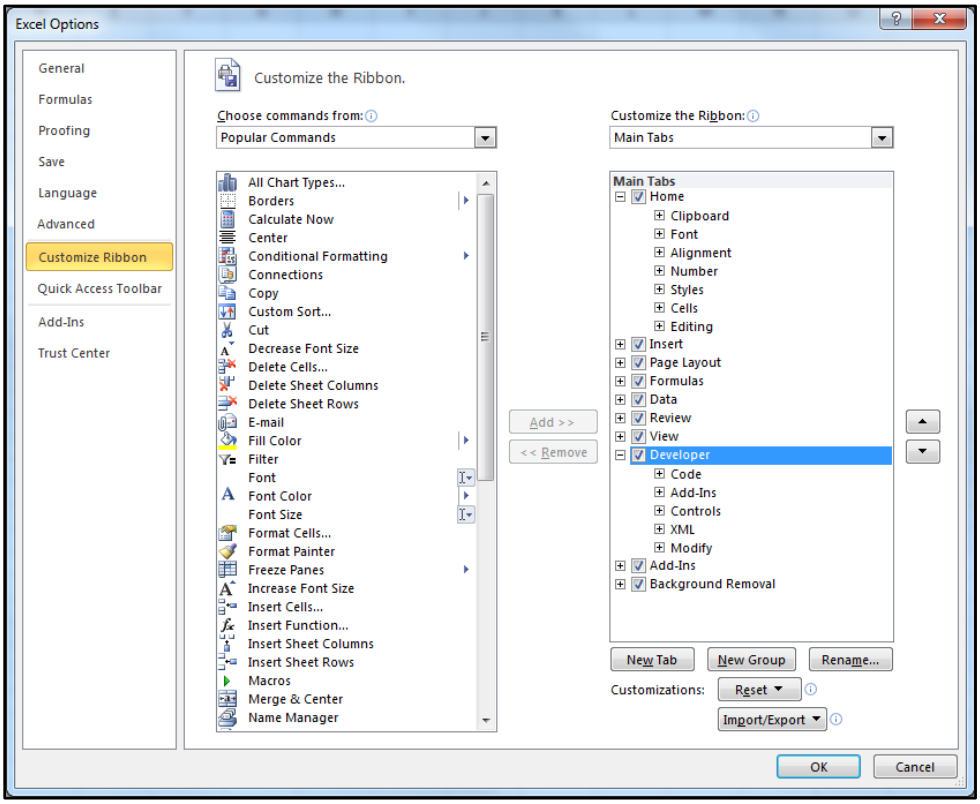


4. Click **Macro Settings** and select the **Enable all macros** radio button.

Excel 2010

1. Right-click the **File** tab and select **Customize the Ribbon**. The **Customize the Ribbon** panel is displayed.

Figure 231: Excel Options screen – Customize Ribbon option



2. Select the **Developer** checkbox in the **Main Tabs** menu, and click **OK**.
   The **Developer** tab should appear at the top of the screen.

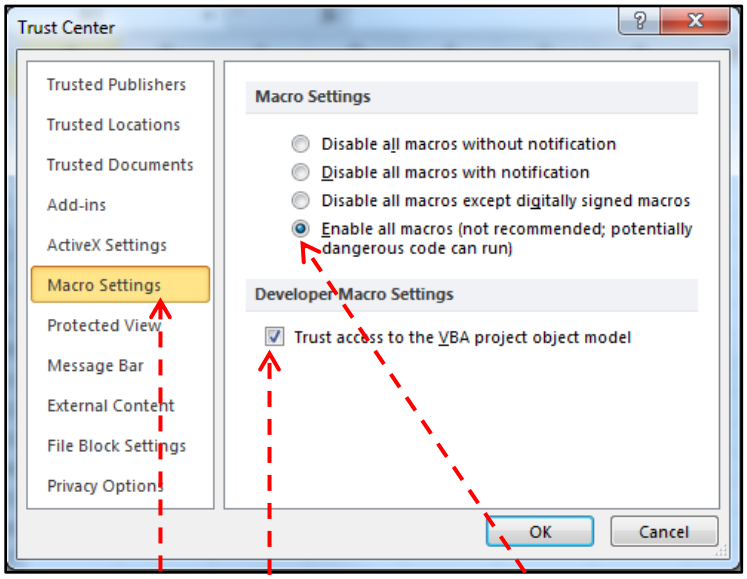
3. Select the **Developer** tab and its **Macro Security** option.

Figure 232: Macro Security option of the Developer panel

   If only a tooltip is displayed, select the **Macro Security** option again.

4. The **Trust Center** dialog box is displayed.

Figure 233: Trust Center dialog box

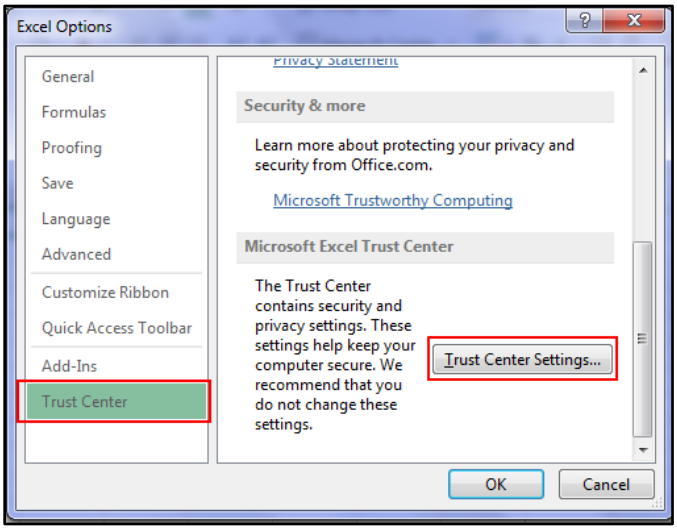


5. In the left panel, select **Macro Settings**, select the **Enable all macros** radio button, and select the **Trust access to the VBA project object model** checkbox.

Excel 2010 and 2013

Method 1

1. Open a Microsoft Excel file, navigate to **File > Options > Trust Center**, and click **Trust Center Settings**.



2. In the **Trust Center Settings** window select **Macro Settings** and select **Enable all macros**.

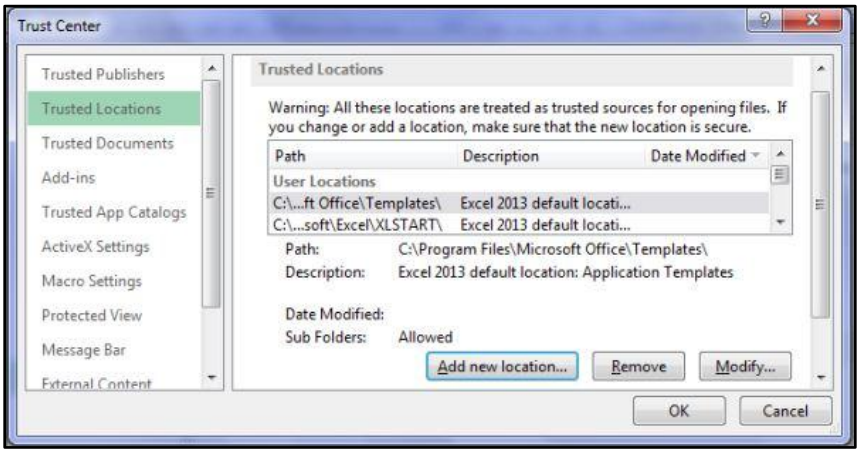
Method 2

Microsoft Excel treats certain paths as trusted zones. If you store an Excel file in one of these trusted paths, Excel will skip macro checks and run the macros. By default, these paths are trusted zones:

- Program Files\Microsoft Office\Templates
- Program Files\Microsoft Office\Office12\Startup
- Program Files\Microsoft Office\Office12\Library
- Program Files\Microsoft Office\Office12\XLSTART

You can make any path a trusted zone by performing these steps:

1. In Excel navigate to File > Options > Trust Center> Trust Center Settings > Trusted Locations



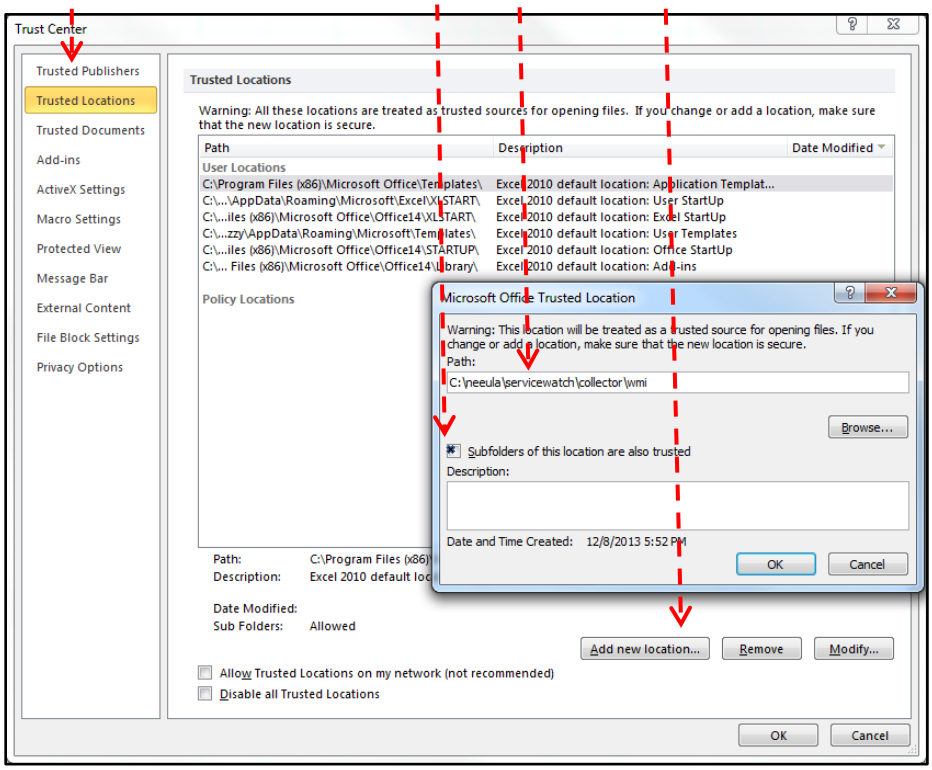
2. Click the **Add new location** button to designate any path as a Trusted Location.

Note: Before adding any location to the trusted location list, ensure the location is really a safe location. These locations can act as security loopholes and a hacker can take advantage of such loopholes.

Configure the WMI collector to execute Excel-reports

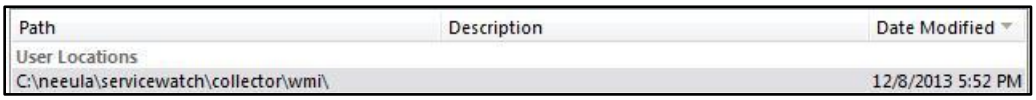
1. Select **Trusted Locations** in the left panel and click the **Add new location** button. In the **Microsoft Office Trusted Location** dialog box, **Browse** to select the path or type in the path to the WMI collector. The default is **C:\neebula\servicewatch\collector\wmi** Change the path if ServiceWatch is not installed on the default path. Select the **Subfolders of this location are also trusted** checkbox. Click **OK**.

Figure 234: Trusted Locations option of the Trust Center screen



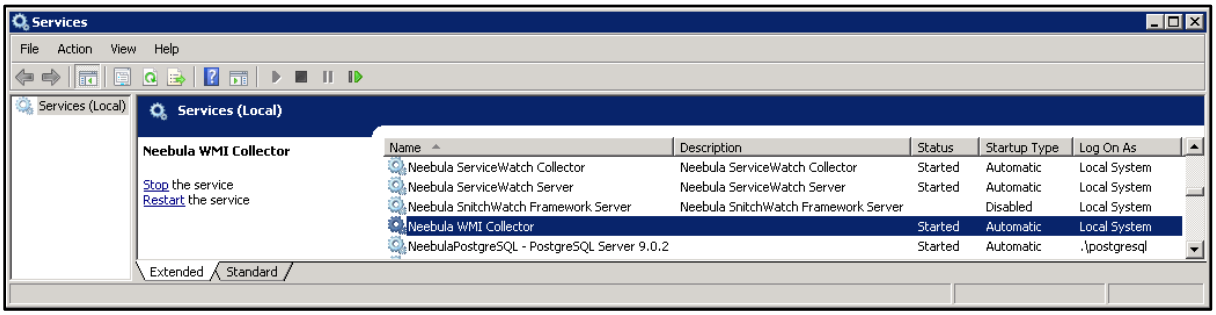
2. Confirm that the new location was added, then click **OK** to exit the **Trust Center** window.

Figure 235: Trusted Locations Path list



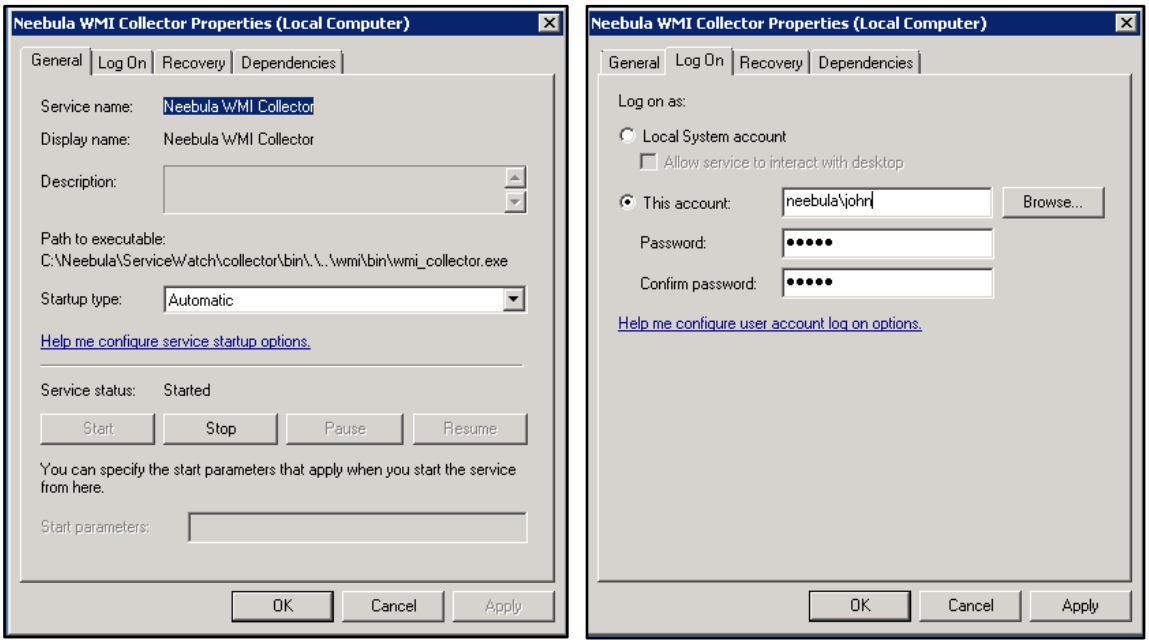
3. Open the Windows **Services** screen of the machine on which the on-site WMI Collector runs and scroll to the row that contains **WMI Collector**.

Figure 236: WMI Collector in the Windows Services screen



4. Right-click this row and select **Properties**. In the **Properties** window, click the **Log On** tab.

Figure 237: Properties window – General panel and Log On panel



5. Select the **This account** radio button and type the same **Domain_name\user_name** and password specified in the **ServiceWatch Credentials** dialog box shown on page 235 or 237 when configuring Excel macro security.

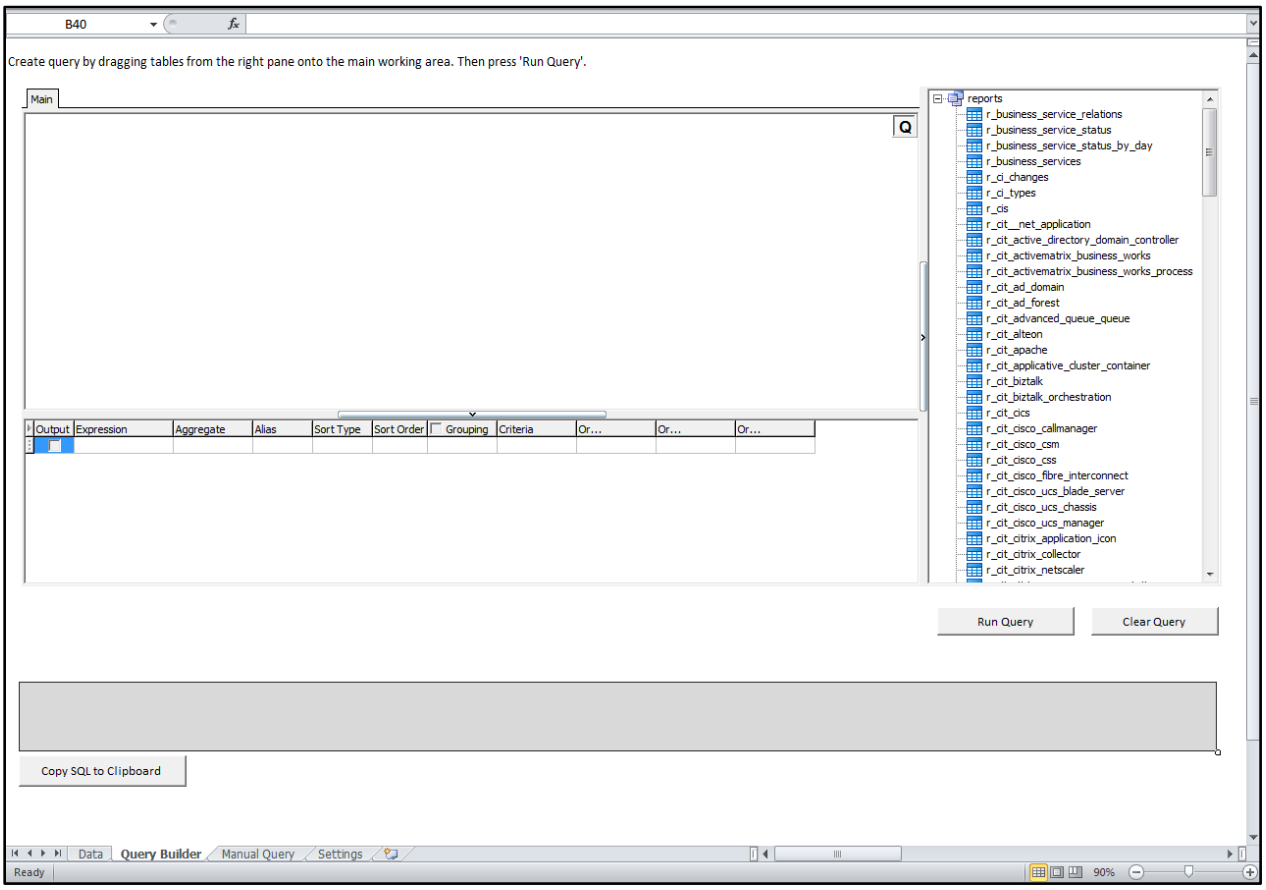
6. Verify that a firewall does not block communication from the ServiceWatch server to the collector machine on **port 8585** and in the opposite direction on **port 8080**.

Using the Excel SQL Query Reports Generator

To design a custom report, run the extracted **ServiceWatch_customized_report.xltm** file. If you receive this Security Warning, click the **Enable Content** button to populate the form.

By default, the *graphic* **Query Builder** tab of the Excel SQL query generator application is displayed:

Figure 238: Graphic SQL Query Builder tab of the Reports Generator Excel application



Appendix B: Schemas for Tables & Views contains a description of every table and every view plus a description of each column header contained in them. The tables contain calculated data that is updated once every 24 hours (at 2 AM by default). The views contain data that is retrieved from ServiceWatch's system tables whose data is always current.

To manually specify the SQL Query for a report, click the **Manual Query** tab at the bottom of the screen.

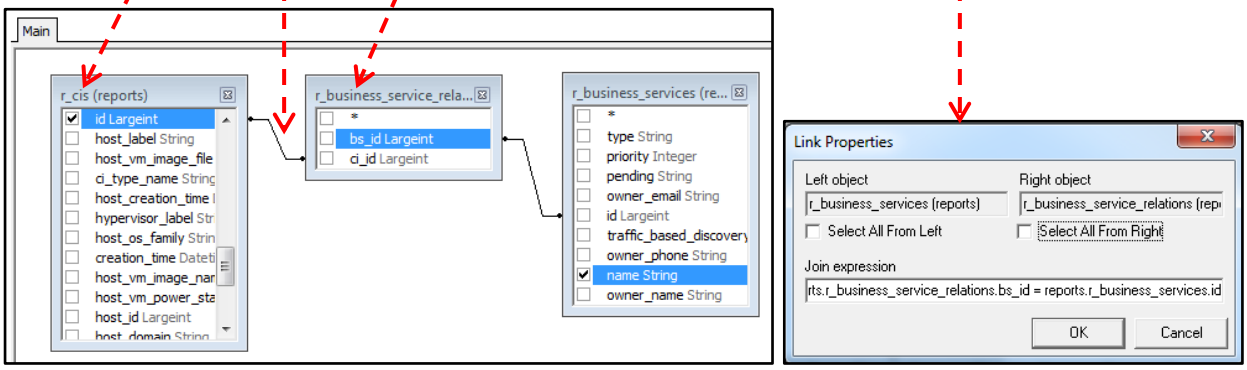
To specify or modify the settings for this application, click the **Settings** tab at the bottom of the screen.

Creating SQL statements graphically

In the **reports** tree in the right panel, double-click the tables and views whose columns contain values that you want to display in the report. The column headers for each selected table or view are listed in the **Main** panel. Use the up and down arrows of each list to display pairs of column headers that create a table 'join' if the values of their rows satisfy the join criterion. The default criterion is EQUALS.

To join analogous headers in two tables, drag one of them to the other. For example, drag **id** from table **r_cis** to **d_id** in table **r_business_service_relations**. Each pair of joined headers is indicated by a double-headed arrow. If you double-click an arrow, its **Link Properties** dialog box is displayed.

Figure 239: Creating links (joins) between database tables & displaying Link Properties



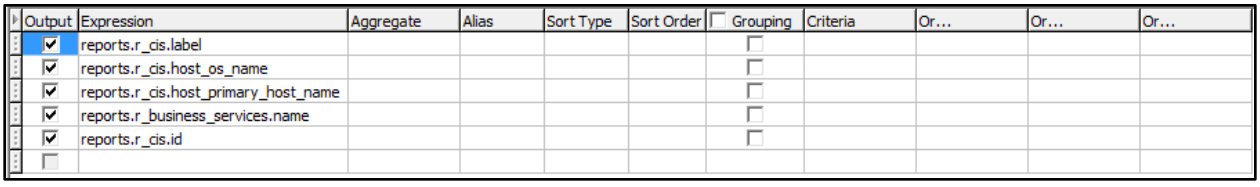
If you select the **Select All From Left** checkbox, the Inner Join SQL string is replaced by a Left Outer Join string. If you select the Select All From Right checkbox, the Inner Join string is replaced by a Right Outer Join string. If you select both checkboxes, the Inner Join string is replaced by a Full Outer Join string. The replacement is performed when you click **OK**.

The Inner Join returns all the columns in both tables but only the rows for which there is an equal value in the join column. The Left Outer Join returns all rows from the left table with the matching rows in the right table. The result is NULL on the right side when there is no match. The Right Outer Join returns all rows from the right table with the matching rows in the left table. The result is NULL on the left side when there is no match. The Full Outer Join returns all rows from both the left and right tables.

Defining columns to be displayed in the Report

Select the checkbox of each header that you want to display in the report. Each selected header is concatenated with 'reports' and the name of its table to form a reports.<table name>.<header> string that is dynamically listed in the **Expression** column in the bottom half of the **Main** panel.

Figure 240: Expression column in the Main panel of the graphic Query Builder



Output	Expression	Aggregate	Alias	Sort Type	Sort Order	Grouping	Criteria	Or...	Or...	Or...
☑	reports.r_cis.label					☐				
☑	reports.r_cis.host_os_name					☐				
☑	reports.r_cis.host_primary_host_name					☐				
☑	reports.r_business_services.name					☐				
☑	reports.r_cis.id					☐				
☐										

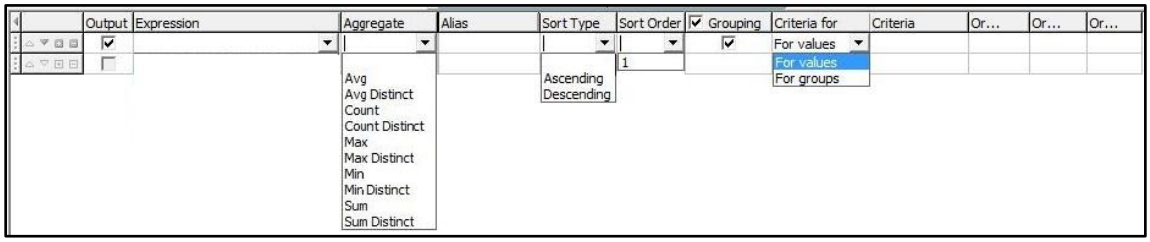
If you click the **Aggregate**, **Sort Type**, or **Sort Order** column of any Expression's row, a down-arrow is displayed. Click that arrow to display a drop-down list of values that can be selected.

If any Expression is Aggregated, **Grouping** checkboxes are automatically selected and a pop-up **Criteria for** column is set to **For groups** or **For values**. If all **Aggregate** values are set to blank,

uncheck the checkbox in the **Grouping** header to uncheck the **Grouping** checkboxes and hide the **Grouping** column.

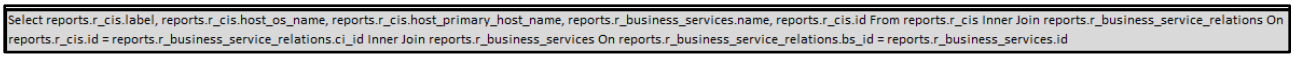
The system may automatically allocate an Alias for an Expression. You can manually assign a unique alias to any Expression. The **Alias** can be used instead of the **Expression** when specifying filter Criteria. If Expression values should be sorted in the report, specify the **Sort Type** (**Ascending** / **Descending**). If you specify a **Sort Type** for more than one **Expression**, the **Sort Order** is automatically set to the sequence in which they were specified. You can change that sequence by clicking the number you want to change.

Filter Criteria can be specified for an **Expression** by selecting **For values** or **For groups** in the **Criteria for** column (if it exists) and specifying a Boolean symbol (for example, =, >, >=) followed by a value in the Criteria column. Only data that satisfies the specified Criteria is displayed in the report.



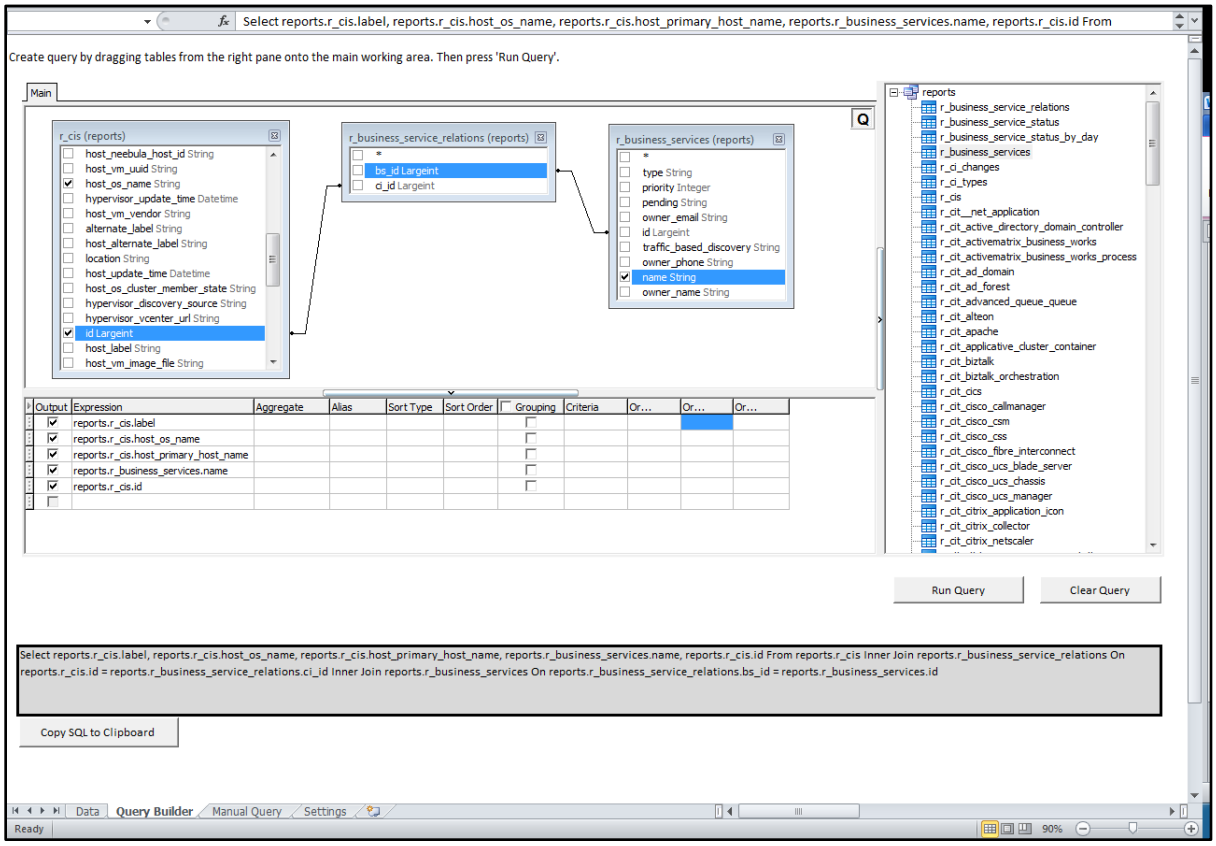
Click the right-arrow in the top left corner of this table to display 4 icons on each row. Click these icons to move a row up, move a row down, delete a row, or undelete a row. Click the left-arrow to hide these icons.

The defined SQL statement is automatically displayed and dynamically modified in the grey textbox.



Sample Query built graphically

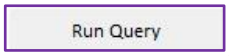
Figure 241: Sample query built graphically

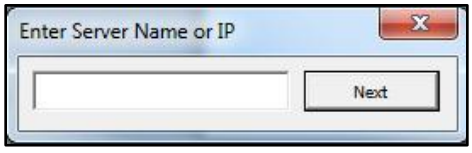


To copy the SQL statement from the textbox to your clipboard, click 

. One reason for doing this is to paste a graphically-built query into the textbox of the Manual Query tab so that a sophisticated SQL user can make complicated modifications that cannot be implemented by the graphical Query Builder.

To erase the contents of the Query Builder textbox *without* running the query, click 

After the query is phrased correctly, click 

, type the Server Name or IP in the 

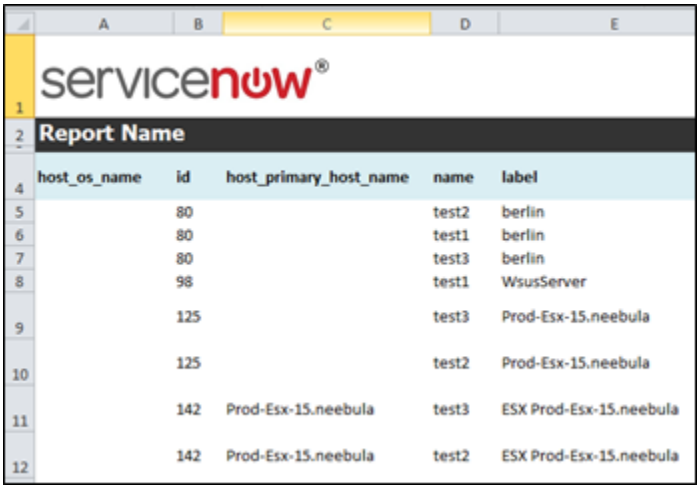
dialog box, and click Next.

ServiceWatch Credentials dialog box

In the **ServiceWatch Credentials** dialog box, enter your **User name** and **Password** and click **Next**.

If the query is valid, the report is generated automatically and displayed in the **Data** tab. You can save the generated report output by selecting **File > Save** or **Save As** in the **Data** tab.

Figure 242: Report Name table in the Data tab



Report Name				
host_os_name	id	host_primary_host_name	name	label
	80		test2	berlin
	80		test1	berlin
	80		test3	berlin
	98		test1	WsusServer
	125		test3	Prod-Esx-15.neebula
	125		test2	Prod-Esx-15.neebula
	142	Prod-Esx-15.neebula	test3	ESX Prod-Esx-15.neebula
	142	Prod-Esx-15.neebula	test2	ESX Prod-Esx-15.neebula

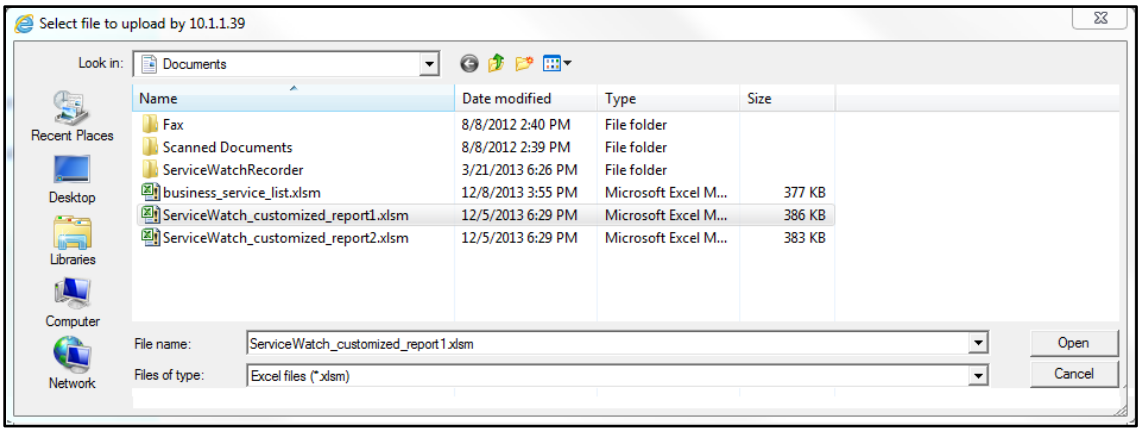
To save the query so it can be uploaded to become a ServiceWatch Saved Report, click **File** > **Save** or **Save As** in the graphic **Query Builder** or **Manual Query** tab.

Uploading an Excel generated Report query

To upload the saved query so the report it generates can be scheduled to run automatically or manually, click 

in the bottom left corner of the ServiceWatch Reports screen.

Figure 243: Select file to upload by <IP address> window

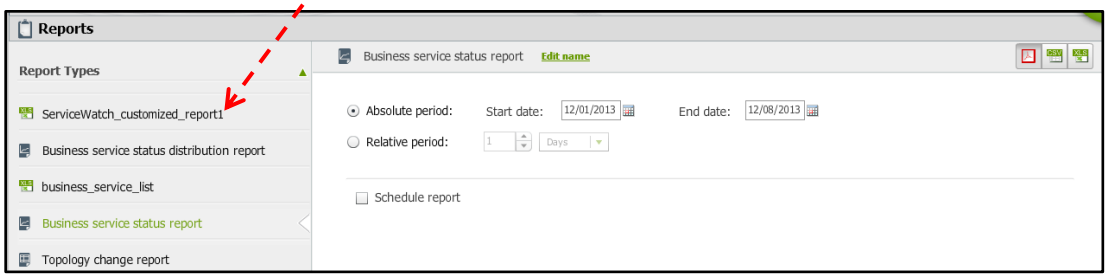


Select the report to upload in the **Select file to upload by <IP address>** window and click Open.

If the Report name in the **Upload a Report** confirmation box is the report you want, click Upload.

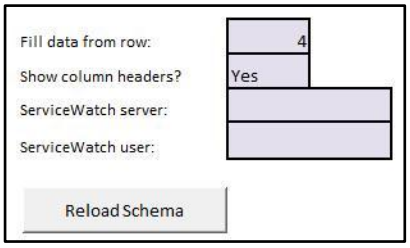
Figure 244: Verification that an uploaded Report is one of the listed Report Types

Verify that the uploaded report is now one of the listed Report Types.



After an Excel report has been uploaded, it can be scheduled exactly like any other report.

Modifying the Report Style



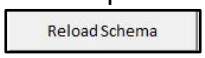
When you click the **Settings** tab, 4 fields for specifying Query Builder schema values are displayed.

Fill data from row defaults to 4 to prevent overwriting the headers.

Show column headers? defaults to Yes.

If ServiceWatch is installed locally, enter its URL in the **ServiceWatch server** field. If only collectors are installed on your system and you access ServiceWatch via the cloud, enter servicewatch.servicenow.com in this field.
Later, this field defaults to the value you entered.

Manually enter the ServiceWatch user name for the first report. Later, it defaults to that value.

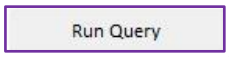
After setting or modifying any schema values, click 

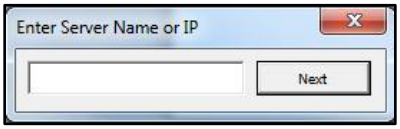
.

Manual Query tab

Click the Manual Query tab to display a large grey textbox where you can type in and modify an SQL query. You can also use the 

button.

After the query is written correctly, click 

, type the Server Name or IP in the 

dialog box, and click Next.

ServiceWatch Credentials dialog box

Figure 245: ServiceWatch Credentials dialog box

In the 

ServiceWatch Credentials dialog box, enter your User name and Password and click Next.

If the query is valid, the report is generated automatically and displayed in the Data tab.

To erase the contents of the Manual Query textbox, click the 

button.

Chapter 13: Troubleshooting

Windows Management Instrumentation (WMI)

0x800706BA – RPC Server Unavailable

This error usually indicates a Remote Procedure Call (RPC) is blocked by a Windows or external firewall.

To verify if a firewall is causing the problem, run the command **`wmic /NODE:target_server_ip_address /user:domain\user /password:xxxx cpu get`** first from the collector machine and then from another Windows machine in same segment as the target server.

From the collector machine you will get the **RPC Server unavailable** message. From the other machine, you may get either a successful result or an **Access Denied** error. In either case, it means there is network blocking between the collector and the target host.

If Windows firewall is working on the target server, disable it temporarily and try again to run the **`wmic`** command from the collector machine. If Windows firewall is not working, the blockage is probably caused by another firewall or router.

Another cause is that the target server has multiple IP addresses and ServiceWatch is listening only to the Application port and not to the full range of ports. RPC initially uses port is 135. Later it uses any port numbered 1024 or higher. In this case, right-click the error and select the **Add Management IP** option.

0x80070005 – E_ACCESS_DENIED

Log in to the relevant server using RDP (Remote Desktop Protocol) to verify that the user name and password you provided are correct.

Access Denied errors can occur even if the user is a local administrator. Verify whether this is the case.

Verify that DCOM (Distributed Component Object Model) is enabled on both the host and the target PC. Check these registry entries on both computers:
Key: **`HKEY LOCAL MACHINE\Software\Microsoft\Ole`**
Name: **`EnableDCOM`**
Type: **`REG_SZ`**
Data: **`Y`**

Verify that WMI is enabled. Check for the presence of WMI by going to the target server, selecting
Start > Run and typing **`wbemtest`**. If the WMI Tester application starts, then WMI is present.

After **wbemtest** starts, click **Connect**, again click **Connect**, then click **Query**. Type **Select * from Win32_ComputerSystem** and click **Apply**. You should get a reply with the computer's name.

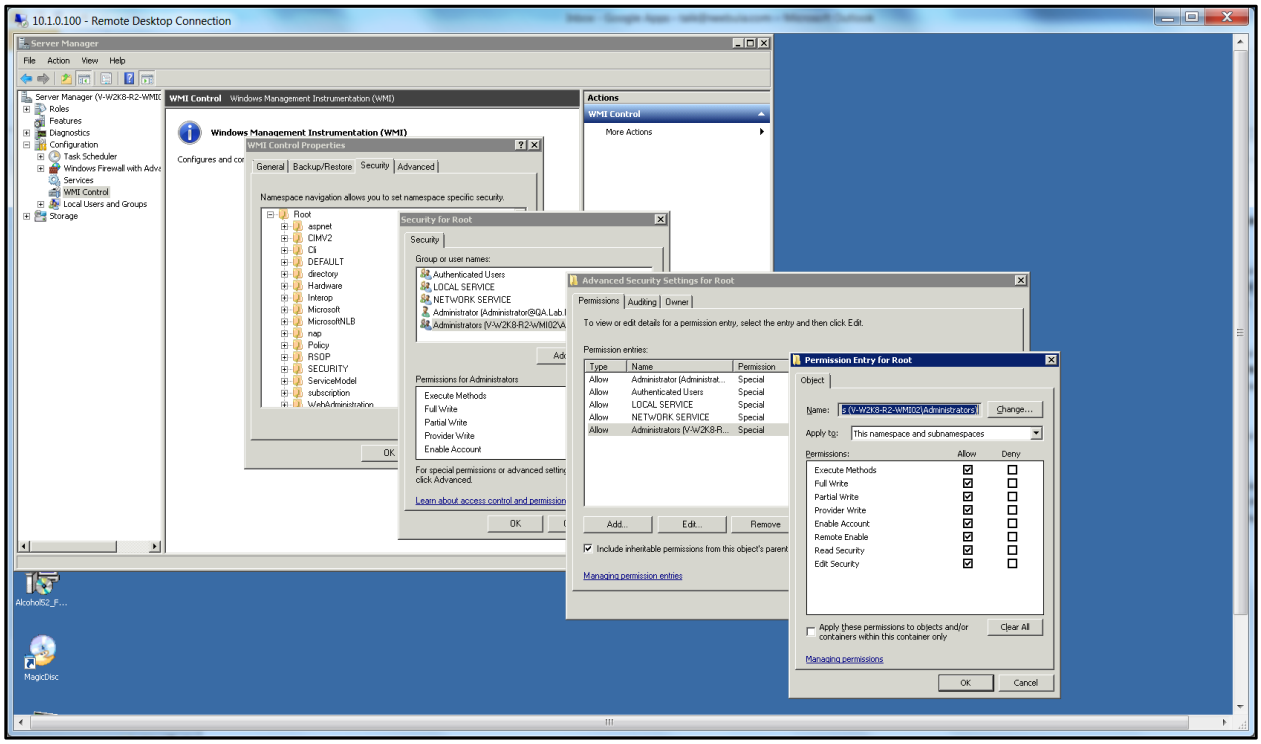
Ensure that remote access and WMI-related services have not been disabled.
The following services should be running or able to start on demand:

- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Procedure Call (RPC)
- Remote Procedure Call (RPC) Locator
- Remote Registry
- Server
- Windows Management Instrumentation (WMI)
- Windows Management Instrumentation Driver Extensions
- WMI Performance Adapter

ServiceWatch failed to run one or more specific commands

In some cases, ServiceWatch may connect to WMI but fail to run a command such as **`netstat`**. The problem is usually that the Administrator group on the machine does not have all of the rights provided by the default Windows installation. In this case, assign the missing rights to the ServiceWatch user.

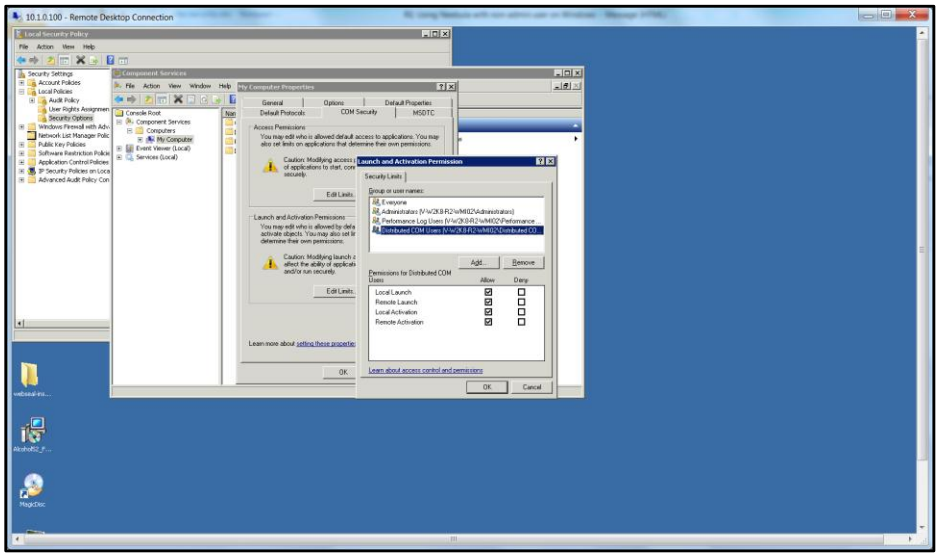
Figure 246: WMI Ctrl > WMI Ctrl Prop. > Security for root > Adv. Security...> Permission Entry...



Verify DCOM Rights

Use **`Dcomcfg.exe`** to verify that the ServiceWatch user (or the group the user belongs to) has full Launch and Activation Permission rights, as seen in Figure 247.

Figure 247: Local Security Policy > Component Serv. > Computer Prop. > Launch & Activation…

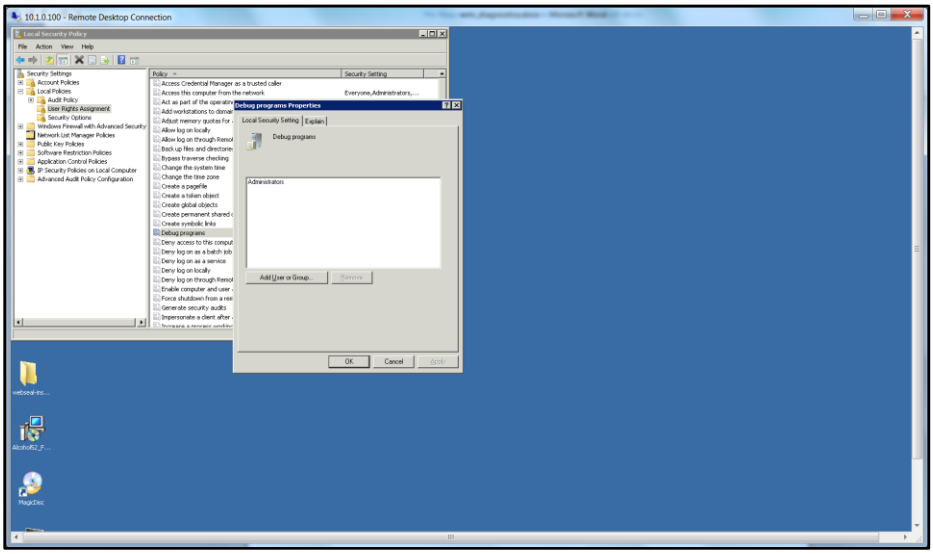


Verify Security Policy

Use **`secpol.msc`** to verify that the ServiceWatch user (or the group the user belongs too) has the following rights:

- Debug Programs
- Restore Files and Directories
- Logon as batch job
- Logon as service

Figure 248: Local Security Policy > Debug programs Properties



Appendix A: Discovery Workflows

The two types of discovery workflows are described below:

- Initial discovery is performed on a business service during its creation/configuration.
- Rediscovery is performed at the frequency (time interval) specified in its skeleton.

Note: Both Initial discovery and Rediscovery can only be performed in a live environment. For example, to perform discovery on a Web Server on a host, the Web Server must be running.

Initial Discovery

Initial discovery is a top-down process that begins with the entry points that are defined in the business service configuration.

An entry point is a pointer to an application on a host. When defining a business service (see CHAPTER 6: CONFIGURING BUSINESS SERVICES), you define the entry point for the top level application in that service. This becomes the starting point from which discovery is performed for that application.

An entry point contains information used during the normal application flow to connect to that application. The type of entry point information required depends on the applications involved.

For example, an Apache to WebSphere entry point could contain URL information.
A WebSphere to WebSphere entry point might contain EJB (Enterprise JavaBean) or WS information.

Initial discovery consists of three basic tasks: identify the host, identify relevant applications, and find outgoing connections.

1. **Identify the host**

Each entry point points to a host computer. For each entry point, initial discovery locates this computer.

2. **Identify relevant applications**

Each entry point type can have certain application types (for example, IIS, Apache, WebSphere) that can apply to it. Using the entry point parameters, discovery looks for and finds relevant application types on the host.

3. **Find outgoing connections**

For each relevant application, discovery finds and follows outgoing connections. Outgoing connections from an application are essentially entry points to the next level. Outgoing connections can belong to the same or a different host and can lead to different applications.

For each connection, discovery repeats the process of identifying the host, finding the relevant applications, and finding more ongoing connections, until there are no more outgoing

connections, or until it can look no farther (for example, because there are credential problems or a connection host computer is not available).

- Discovery can determine if objects constitute an Applicative cluster. An Applicative cluster is a group of applications that serve the same purpose or functionality for the business service. For example, 10 web servers available for the same purpose and used for load balancing would constitute an Applicative cluster.
- In a topology, all the objects in the cluster appear as individual icons within a frame that encloses the cluster.
- When discovery encounters a problem, a discovery error is issued and displayed in the topology:
  - ✓ Some problems can be fixed in the Topology Map (for example, by adding credentials or marking as a boundary).
  - ✓ Some problems are corrected by an external fix. For example, if a particular computer required for discovery is down, to fix the problem you should bring up that computer.
- You can adjust the topology whether or not discovery issues an error. For example:
  - ✓ If you determine that an object and its connections are not part of your business service, you can mark a boundary at the top of that part.
  - ✓ If a connection is missing, you can manually add it.

Note: When you add a connection, ServiceWatch automatically continues discovery on that connection.

Rediscovery

Rediscovery is performed on a business service after the business service is activated. Most aspects of Initial Discovery and Rediscovery are the same. The main differences are:

- Each CI in the business service Map is rediscovered based on its own frequency schedule. If you select a CI in **Edit** mode, you can change its rediscovery frequency.
- If an existing CI stops being discovered, the system does not immediately remove that CI and its descendant CIs. The connection is removed only after the **Regular connection aging time in minutes** specified in the **Rediscovery** section of the **Global Parameters** window has elapsed.
- During most rediscovery cycles, the system runs only those patterns that executed successfully during initial discovery plus some patterns that were found during a rediscovery. However, the system runs a 'full rediscovery' (meaning it runs all relevant patterns) during every Nth cycle where N is the value specified for the **Full rediscovery every N times** global parameter.

Appendix B: Schemas for Tables & Views

This appendix lists built-in table and view schemas that can be used for ServiceWatch reports. The Name of each table is **purple**, the Name of each view is **blue**, and their columns are listed under their Names.

Table data is updated once every 24 hours. By default, data is updated at 2 AM every night. View data is always current because it is updated automatically immediately prior to its usage.

Table 11: Built-in Schemas for ServiceWatch Reports

Table *or* **View** / Column Header	**Description**
r_business_service_relations	Relation between CIs and business services
Ci_id	CI identifier
Bs_id	Business service identifier
r_business_service_status	Severity (CRITICAL, MAJOR, etc.) status over time
ID	Business service identifier
Name	Business service name
Priority	Business service priority
Type	REGULAR *or* TBS (Technical Business Service)
Is_pending	Business service state = Pending? TRUE *or* FALSE
From_time	Time when a business service status began
To_time	Time when a business service status ended
Severity	Business service severity status: 0 – INFORMATION 1 – MINOR 2 – WARNING 3 – MAJOR 4 – CRITICAL
r_business_service_status_by_day	Time intervals when a business service was not in INFORMATION status each calendar day. Each row indicates the decimal fraction of the day the business service had a certain status. Use this data to create reports that show the total time a business service was in each status during any time period.
Id	Business service identifier
At_year	4-digit Year
At_month	Month (1 to 12)
At_day	Day of month (1 to 31)
Name	Business service name
Priority	Business service priority
Type	REGULAR *or* TBS Technical Business Service)
severity	Business service severity: 0 – INFORMATION 1 – MINOR 2 – WARNING 3 – MAJOR 4 – CRITICAL
Part_of_day	Decimal fraction of the day (from 0.0000 to 1.0000) during which a business service was in that status.

Table *or* View / Column Header	Description
r_business_services	Attributes of each business service
id	Business service identifier
Name	Business service name
type	REGULAR *or* TBS (Technical Business Service)
Priority	Business service priority
Pending	Business service state = Pending? TRUE *or* FALSE
owner_email	Email of business service owner
Owner_name	The business service owner name
Owner_phone	Phone number of business service owner
Traffic_based_discovery	For internal use by ServiceWatch
r_ci_changes	Changes detected in CIs over time
Ci_id	Identifier of the configuration item
Changes	Description of the change
Time	Date & time (user format) when a change occurred
r_ci_types	List of all CI types available in ServiceWatch
Ci_type_id	CI type identifier
Ci_type_name	CI type internal name
Display_name	Name of CI type displayed in the user interface
Category	Parent category of CI type (e.g., Application Servers, Web Servers)
r_cis	List of all CIs detected by ServiceWatch
Id	CI Identifier
Location	Editable attribute
Label	Label assigned by the system
Alternate_label	Label assigned by a user
Discovery_source	Process that created this CI
Creation_time	Date & time this CI was created in ServiceWatch
Update_time	Last date & time CI was updated in ServiceWatch
Ci_type_name	Name of the CI type
HOST COLUMNS	All columns of the r_hosts view of this CI's host. If this CI is a host, those columns are empty.
r_cit_<name of the CI type> For example: **r_cit_apache**	The view name starts with **r_cit_** and continues with a CI type name. All characters are lower case and consecutive spaces are replaced by 1 space.
Id	CI identifier
Apache_label	Label assigned by the system
Apache_alternate_label	Label assigned by user

Table *or* View / Column Header	Description
Apache_location	Editable attribute
Apache_discovery_source	Process that created this CI
Apache_creation_time	Date & time this CI was created in ServiceWatch
Apache_update_time	Last date & time CI was updated in ServiceWatch
Apache_software_version	Apache version
Apache_configuration_file	Location of Apache configuration file
Apache_home_directory	Home directory of Apache
HOST Columns	All columns of the r_hosts view of this CI's host
r_connection_types	List of all available connection types
Id	Connection type identifier
Name	Name of the connection type
Category	Values: NETWORK, APPLICATION_FLOW, INCLUSION, STORAGE_FLOW, INTERNAL
Hidden	Is connection type shown in the map? True *or* False
Display_name	Name displayed in the user interface
Description	Description of the connection type
r_connections	Lists all connections in the system. The following connections (which describe relationships between CIs) are listed: INCLUSION – a parent (e.g., WebSphere) – child (e.g., WebSphere EAR) relation. APPLICATION_FLOW – a data-flow connection between 2 CIs in a business service CLUSTER – cluster controller (e.g., load balancer) – cluster member connection CLUSTER_MEMBER – an internal CI (an applicative_cluster) – member connection STORAGE_FLOW – connections between applications (e.g., PostgreSQL database) – and file systems – connections between a host and fiber channel switches or storage arrays. NETWORK – connects host – network switch, network switch – switch or router, etc. INTERNAL – internal usage (used by ServiceWatch but not meaningful to a customer)
Source_ci_id	Source CI identifier
Target_ci_id	Target CI identifier
Connection_category	INCLUSION, APPLICATION_FLOW, CLUSTER, CLUSTER_MEMBER, STORAGE_FLOW, NETWORK, INTERNAL
Type	Entry point types in the knowledge base, e.g., HTTP(S), TCP.
r_errors	Message logs for discovery and other system processes
Id	Internal identifier
Timestamp	Time the message was created
Status	For internal use
Stacktrace	Software stack trace associated with the message
Category	Message category

Table *or* **View** / Column Header	**Description**
Task_type	Type of the task that generated the message, e.g., INITIAL_DISCOVERY, REDISCOVERY
Bs_id	Business service ID associated with the message
Conn_id	Connection ID associated with the message
Ci_id	CI identifier associated with the message
Ip	IP address of host associated with the message
Task_origin	Type of process that triggered this message
Error_id	ServiceWatch error code, e.g. NBL-1024, NBL1043
Message	Full text of the error message
Connection_section_name	Name of connection section in message's pattern
Step_name	Name of the step in the message's pattern
Identification_section_name	Name of the ID section in the message's pattern
Pattern_id	ID of the pattern associated with the message
Host_id	ID of the host associated with the message
Detailed_message	For future use
r_events	All active and closed events in the system
Id	Event internal identifier
Priority	See Event Priority on page 43
Hostaddress	Address/name of host the event is associated with
Citypename	Name of the CI type if event is for a specific CI type
Businessservicename	Business service (BS) monitor name for BS events
Severity	0-INFO,1-WARN,2-MINOR,3-MAJOR,4-CRITICAL
Text	Event text
Params	Event parameters
Bindingruleid	ID of event's binding rule. Not always populated
Emssystem	Name of monitoring system that generated event
Messagekey	Identifier of the event used in order to close events
Creationtime	Date and time the event was created
Lastchangetime	Last time event (or its severity) was changed
Neebulaclosetime	Time the event was closed
Status	Values: active *or* closed
r_history_changes	Changes detected in a business service over time
Bs_id	Business service ID
Changes	Text description of the change
Time	Time of the change

Table *or* View / Column Header	Description
r_hostnames_ip_addresses	All IP addresses and host names in the database
Host_id	Corresponds to ID field in r_hosts, r_servers & r_cis
Ip_address	IP address of this host
Host_name	Host name that corresponds to the IP address
r_hosts	All detected hosts incl. servers and network devices
Host_id	Configuration item ID of this host
Host_os_family	Operating sys.: WINDOWS, UNIX, PROPRIETARY
Host_os_type	Operating system type, e.g., WINDOWS_2008
Host_serial_number	Serial number of the host
Host_model	Model of the host
Host_location	Editable attribute
Host_label	Label assigned by the system
Host_alternate_label	Label assigned by a user
Host_vm_image_file	VM image file name (relevant for VmWare)
Host_vm_cpu_number	Number of VM CPUs (relevant for VmWare)
Host_vm_vendor	Vendor of the virtualization platform
Host_vm_power_status	E.g., poweredOn, poweredOff
Host_vm_vcenter_url	URL of vCenter managing this host (for VmWare)
Host_vm_memory_mb	VM memory (relevant for VmWare)
Host_vm_image_name	Virtualization image name
Host_hypervisor_address	Address of hosting hypervisor
Host_primary_host_name	Primary host name
Host_primary_management_ip	Management IP of this host
Host_os_version	Operating system version
Host_address_width	32 bit or 64 bit platform
Host_neebula_host_id	Internal attribute
Host_vm_uuid	Universal unique identifier of the virtual machine
Host_discovery_source	Process that discovered this host
Host_creation_time	Date & time host was created in ServiceWatch
Host_update_time	Last date & time host was updated in ServiceWatch
r_hypervisors	Virtualization container types detected,AIX HMC etc
Hypervisor_id	Configuration item ID of this hypervisor
Hypervisor_vendor	Vendor of the virtualization platform, e.g., VmWare
Hypervisor_location	Editable attribute. Default: null
Hypervisor_label	Label assigned by the system
Hypervisor_alternate_label	Label assigned by a user
Hypervisor_product_name	Name of product, e.g., ESX for VmWare
Hypervisor_full_name	For example, VmWare ESX 4.0.0 build 201487

Table *or* View / Column Header	Description
Hypervisor_vcenter_url	Vcenter URL for this hypervisor (for VmWare)
Hypervisor_version	Hypervisor product version
Hypervisor_discovery_source	Process that discovered this hypervisor
Hypervisor_creation_time	Date & time this CI was created in ServiceWatch
Hypervisor_update_time	Date & time this CI was updated in ServiceWatch
r_servers	All servers detected by ServiceWatch
Host_id	Configuration item ID of this host
Host_os_family	Operating sys.: WINDOWS, UNIX, PROPRIETARY
Host_os_type	Operating system type, e.g., WINDOWS_2008
Host_serial_number	Serial number of the host
Host_model	Model of the server
Host_location	Editable attribute
Host_label	Label assigned by the system
Host_alternate_label	Label assigned by a user
Host_vm_image_file	VM image file name (relevant for VmWare)
Host_vm_cpu_number	Number of VM CPUs (relevant for VmWare)
Host_vm_vendor	Vendor of the virtualization platform
Host_vm_power_status	E.g., poweredOn, poweredOff
Host_vm_vcenter_url	URL of vCenter managing this server (for VmWare)
Host_vm_memory_mb	VM memory (relevant for VmWare)
Host_vm_image_name	Virtualization image name
Host_hypervisor_address	Address of server hypervisor
Host_primary_host_name	Primary server name
Host_primary_management_ip	Management IP of this server
Host_os_version	Operating system version
Host_address_width	32 bit or 64 bit platform ?
Host_neebula_host_id	Internal attribute
Host_vm_uuid	Universal unique identifier of the virtual machine
Host_discovery_source	Process that discovered this server
Host_creation_time	Date & time server was created in ServiceWatch
Host_update_time	Last date & time ServiceWatch updated this server

Appendix C: Glossary

Table 12: Glossary

Term	Description
A	
AD Domain / Forest	Active Directory Domain / Forest
Alteon Load Balancer	Load Balancing
AMAZON_AWS	Amazon Web Services
Apache Web Server	Apache Web Server guide
apikey	Application programming interface key
Application Cluster	Because servers can easily be added or removed from the cluster as needs dictate, an **application cluster** is more scalable than its hardware-based counterpart. See RAC.
Applicative cluster	A group of applications that serve the same purpose for a business service. For example, 10 web servers that are all used for load balancing constitute an applicative cluster. Objects in a topology that constitute an applicative cluster are enclosed in a box.
Applicative credential type	The Applicative credential type is used for discovering an application or for using an application to discover a connection.
AWS	Amazon Web Services (AWS) is a cloud computing platform offered over the Internet by Amazon.com. Its services include Amazon Elastic Compute Cloud (EC2) and Amazon S3 (Simple Storage Service).
B	
bash script	A bash script is a file containing a list of commands to be executed by the bash shell. Very simple scripts contain a set of commands that you would normally enter from the keyboard. For example, sudo bash ./install.sh
BEA Tuxedo	PeopleSoft Application Server
Big-IP GTM	F5 Network Big-IP Global Traffic Manager data sheet
Big-IP LTM	F5 Network Big-IP Local Traffic Manager data sheet
Binding rules	Binding rules connect source fields and values to transformation targets and fields.
BizTalk Orchestration	Represents the underlying logic for processing messages and provides a transactional programming model that supports exception handling and recovery from failed transactions. BizTalk Orchestration.
BizTalk Server	BizTalk Server uses AS2-to send, receive, encrypt, decrypt, sign, and

	verify messages using HTTP over the Internet. It supports encryption keys, digital signatures, certificates, non-repudiation and other industry standards like RosettaNet, SWIFT, HL7, HIPAA, etc.
C	
CA	Certificate Authority or Certification Authority that issues digital certificates.
CA eTrust Directory Server	CA Directory overview article
CA Introscope	A component of the CA Application Performance Management solution.
CA Policy Server	CA SiteMinder Policy Server Administration Guide, Configuration Guide, and Installation Guide
CI	Configuration Item
CI type	Type of configuration item, usually indicated on topology maps
CICS	Customer Information Control System is a transaction server that runs on IBM mainframes under z/OS and z/VSE. CICS is middleware that supports rapid, high-volume online transaction processing.
CICS Transaction Gateway	Provides access from Java Client applications to CICS applications, using standard Internet protocols. CICS Transaction Gateway
Cisco CallManager	Cisco CallManager Basic Concepts
Cisco CSM	Cisco Security Manager
Cisco CSS	Cisco Content Services Switch
Cisco Fabric Interconnect	Configuring the Fabric Interconnects
Citrix NetScaler	Citrix NetScaler Cloud Network Platform
Citrix XenApp	See XenApp or Presentation Server EP, an on-demand application delivery solution that allows apps to be virtualized, centralized and managed.
CLI	Command Line Interface
CLI Event Sender	When triggered by an alert, this executable sends an event to the ServiceWatch server.
cmdb	Configuration Management Database
Collector	ServiceWatch submits discovery information requests (collection tasks) about machines, applications, hosts, network components, etc. to collectors. The collectors collect the information for ServiceWatch to analyze and use.
Connect-It Service	Version 3.70 User's Guide. Version 4.10 User's Guide.
Control-M Enterprise Manager/Gateway/Server	Wikipedia article. Enterprise Manager. Server Administrator Guide.
CSR	Certificate Signing Request

curl program	**curl** transfers data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP). See http://curl.haxx.se/docs/manpage.html
D	
DataPower	Self-balancing and intelligent load distribution for application servers. For example, IBM WebSphere DataPower SOA Appliances. See DPT.
DB2 Database Server	IBM DB2
DB2 UDB	DB2 Universal DataBase, an enhanced version of DB2 that combines relational and object database technology as well as various query optimization techniques for parallel processing.
DCOM	Distributed Component Object Model is a proprietary Microsoft technology for communication among software components across networked computers. DCOM, which originally was called 'Network OLE',', extends Microsoft's COM and provides the communication substrate under Microsoft's COM+ application server infrastructure.
Debian GNU/Linux	Debian is a free operating system that uses the Linux kernel but most of the OS tools come from the GNU project; hence the name GNU/Linux.
DMZ	A **Demilitarized Zone** is a physical or logical subnetwork that provides an organization's external services to a larger untrusted network, usually the Internet. The DMZ adds an additional layer of security to an organization's local area network. An external attacker can only access objects in the DMZ and cannot access any other part of the network.
Documentum	Brava! Enterprise Webtop Server/Job Processor ver. 6.5 Brava Enterprise ver. 7.0 Architecture Content Server Administration and Configuratiion Guide
Domain Controller	Domain controllers in your network store user account information, authenticate users, and enforce security policy for a Windows domain.
DPT	Data Power Technology. Email: info@datapowertech.com
E	
ECC	EMC Control Center, an application for a storage device from EMC.
EJB	Enterprise JavaBeans
EMC	EMC[2]
EMS	Enterprise Message Service, a Java Message Service by Tibco Software Event Monitoring System
emsEventID	Unique EMS system id for the event, used when the event is bound to

	more than one CI. It can currently be the same as messageKey.
entry point	An entry point is a pointer to an application on a host and the starting point from which Discovery is performed. Each business service must have at least one entry point.
ESB	Enterprise Service Bus
escalationFlag	Values: NORMAL, ESCALATED, ESCALATED_LEVEL2, ESCALATED_LEVEL3, SUPPRESSED
ESX	VMware ESX and ESXi are VMware's enterprise software Type 1 hypervisors for guest virtual servers; they run on hostserver hardware without an underlying operating system.
expireTime	Expiration time
F	
Fast Index Server	Documentum Full Text Index Server
FTP(S)	File Transfer Protocol [with support for Transport Layer Security (TLS) and Secure Sockets Layer (SSL) cryptographic protocols]
G	
Generic Application	Microsoft Generic Application
GNU wget	See wget in this glossary.
GROUNDWORK	GroundWork provides an open software platform for easy integration and customized visualization of cloud, virtualization, network, application, server, and storage data.
H	
HIPAA	Health Insurance Portability and Accountability Act
Hitachi Data Systems	See also Hitachi Storage systems
HL7	Health Level 7
hostAddress	Hostname or IP where a CI (to which an event should be bound) runs.
HP BTO	IT management software, aka Business Technology Optimization (BTO) software, is the largest category of software sold by HP.
HP EVA	See the HP EVA P6000 Storage data sheet
HP OpenView	In 2007, HP OpenView was rebranded as HP BTO (Business Technology Optimization) Software.
HP Operations Manager	A software agent installed on monitored hosts sends selected alerts in 'agent push' mode to a central Management Server. The agent

	classifies each event before transmission. The server routes the messages to destinations that can include operator consoles, trouble-ticket systems, and notification systems.
HP Quality Center	HP Quality Center is quality management software from Hewlett-Packard with capabilities acquired from Mercury Interactive Corp. HP Quality Center provides requirements & test management and business process testing for IT and application environments.
HP SM Index Server	HP Service Manager
HP uCMDB	See Make Your HP uCMDB Service Aware and its Wikipedia article.
HPOM	HP Operations Manager
http	Hypertext Transfer Protocol. See http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
HTTP Listener to WMB Dependency	HTTP Listener to WebSphere Message Broker
HTTPS	HTTP Secure protocol
hypervisor	A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines.
I	
IBM CICS	See CICS.
IBM Tivoli Netcool	See Netcool
IBM WebSphere Message Broker	Lightweight, advanced ESB that integrates data sources from a wide range of platforms across SOA and non-SOA environments.
IBM WebSphere MQ Queue	WebSphere Message Queue
IBM WMB Http Listener	WebSphere Message Broker http listener (see HTTP Listener to WMB Dependency)
IIFP Entry Point	Identity Integration Feature Pack
IIS Website	Internet Information Services
IMAP	Internet Message Access Protocol
Inetinfo	User-mode component that hosts the IIS metabase and the non-Web services of IIS.
iPlanet	A product brand used jointly by Sun Microsystems and Netscape Communications Corporation when delivering software and services as part of a non-exclusive cross marketing deal.
ISA Server	ISA Server and http://www.isaserver.org/
ISAM	*Indexed Sequential Access Method*, a method for indexing data for fast retrieval. Originally developed by IBM for mainframe computers.

J	
Java KeyStore	A Java KeyStore (JKS) is a repository of security certificates, either authorization certificates or public key certificates, used in SSL encryption.
JAXB	Java Architecture for XML Binding
JBoss AS	JBoss Application Server. JBoss is a division of Red Hat.
JDBC	Java Database Connectivity is an industry standard for connectivity between Java programs and databases, spreadsheets and flat files. JDBC provides a call-level API for SQL-based database access.
Jetty	Jetty is a pure Java-based HTTP (Web) server and Java Servlet container.
JIRA	Project and issue tracking software by Atlassian
JMS	Java Message Service http://en.wikipedia.org/wiki/Java_Message_Service
Jrun WAR	JRun provides auto and hot deploy features for dynamic deployment of web applications (WAR file or directory), enterprise applications, and other J2EE modules, such as EJBs & enterprise resource adapters.
JSSE	Java Secure Socket Extension provides a set of packages which enable secure Internet communications. It implements a Java version of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. It includes functionality for data encryption, server authentication, message integrity, and optional client-authentication.
K	
Kerberos	Kerberos is a computer network authentication protocol that uses 'tickets''tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
KeyStore	A **Java KeyStore** is a repository of security certificates used for instance in SSL encryption. In Oracle WebLogic Server, a file with extension *jks* is the keystore. The Java Development Kit maintains a CA keystore in folder jre/lib/security/cacerts. JDKs provide a tool named *keytool* to manipulate the keystore. *keytool* cannot extract the private key out of the keystore, but this is possible with 3rd-party tools like jksExportKey, CERTivity, Portecle and KeyStore Explorer.
KPI	Key Performance Indicator
L	

LDAP	Lightweight Directory Access Protocol
LDAP Database	LDAP Concepts and Overview
Load Balancing	Load Balancing and Load Balancing
M	
MAPI	Messaging Application Programming Interface
messageKey	Unique identifier for a message. When a new event with the same messageKey arrives, the old active event is closed.
MOM	Microsoft Operations Manager. See http://msdn.microsoft.com/en-us/library/aa505337.aspx
MQ	IBM WebSphere Message Queue middleware for messaging across multiple platforms
MQ Flow	WebSphere MQ server-agent workflow
MySQL Cluster Data Node	MySQL Cluster
MS SQL Database	MS SQL Database tutorial; also see MS SQL Server
MS SQL Server	Microsoft RDBM
MSMQ Flow	MS Message Queue flow http://technet.microsoft.com/en-us/library/cc723251.aspx
MySQL Cluster	MySQL Cluster
MySQLClusterDataNode_ EntryPoint	Defining MySQL Cluster Data Nodes
MySQLClusterMGM_ EntryPoint	MySQL Cluster Management Server MySQL Cluster Management Client
MySQLServer_EntryPoint	MySQLServer
MySQLSlaveServer_EntryPoint	MySQL Server replication
N	
Nagios	An open source network infrastructure monitoring system. Due to trademark problems, the original name, *NetSaint*, was changed to *Nagios*, an acronym for 'Nagios Ain't Gonna Insist On Sainthood.'
NAT	Network Address Translation
nblevent	ServiceNow-supplied CLI (Command Line Interface) Event Sender utility. On Windows, the path for nblevent.exe is <*ServiceWatchServer*>\event_cli\bin\ On Unix, nblevent is a shell script with path <*ServiceWatchServer*>/event_cli/bin/
Netcool	IBM-Tivoli Netcool delivers near real-time, consolidated event

	management across business infrastructure, data centers, complex networks and IT domains.
netstat	**netstat** (**net**work **stat**istics) is a command-line tool that displays network connections, routing tables, and network interface (network interface controller or software-defined network interface) and network protocol statistics. It is available on Unix-like operating systems including OS X, Linux, Solaris, and BSD, and is available on Windows NT operating systems including Windows XP, Windows Vista, Windows 7 & 8. It finds problems in the network and determines the amount of traffic on the network as a performance measurement.
NNTP	Network News Transfer Protocol
NTLM	NT LAN Manager is a Microsoft Windows security protocol that can be used where a domain controller is not available or is unreachable. For example, NTLM could be used if a client is not Kerberos capable, the server is not joined to a domain, or the user is remotely authenticating over the web. However, Microsoft no longer recommends using NTLM.
O	
OpenSSL	OpenSSL is a toolkit implementing SSL v2/v3 and TLS protocols with full-strength cryptography world-wide.
Oracle Advanced Queue	Oracle Advanced Queuing
Oracle App TNS service	Name by which an Oracle database is known on a network
Oracle Concurrent Server	Concurrent parallel processing
Oracle Database Schema	Oracle Database Schema
Oracle DB	Oracle Database
Oracle Discoverer Engine / UI	Overview of Oracle Discoverer
Oracle E-Business Suite	Overview of Oracle E-Business Suite
Oracle ESB Connection	Oracle Enterprise Service Bus
Oracle Forms Engine / UI	Oracle Forms is a component of Oracle Fusion Middleware
Oracle Fulfillment Server	Oracle Fulfillment Implementation Guide
Oracle HTTP Server	Web server based on the Apache HTTP Server
Oracle iAS Module INC	iAS configuration and tuning
Oracle Linux	Oracle Linux, formerly known as Oracle Enterprise Linux, is a Red Hat Enterprise Linux freely distributed by Oracle under the GNU General Public License (GPL).
Oracle Listener	Oracle Net Listener is a process that runs on the database server computer. It receives incoming client connection requests and manages the traffic of these requests to the database server.

Oracle Notification Server	See Oracle Process Manager and Notification Server
Oracle Metric Server / Client	Components of the Application Tier used for load balancing.
Oracle OACORE Server	Used to provide core functionality in Oracle E-Business Suite application tier Java code, including OAF-based functionality for Oracle E-Business Suite products.
Oracle OAFM Server	Oracle Apps Fusion Middleware server runs web services, MapViewer, ASControl, and Oracle Transport Agent XML transactions
Oracle Process Manager	Oracle Process Manager and Notification Server
Oracle RAC DB	Oracle Real Application Clusters database
Oracle Reports Server	Configuring the Oracle Reports Server
Oracle Tnslsnr Engine	TNS Listener, starting and stopping
Oracle WebLogic JMS queue	Oracle WebLogic Java Message Service queue
P	
PEM format	Privacy Enhanced Mail (PEM) is a 1993 IETF proposal for securing email using public-key cryptography.
PeopleSoft Application Server	See BEA Tuxedo
Policy Server	Network Policy Server
POP3	Post Office Protocol
PostgreSQL database	PostgreSQL database Open-source object-relational DBMS supporting SQL constructs incl. subselects, transactions, and user-defined types.
Q	
R	
RAC	Real Application Cluster enables a database to be installed across multiple servers. RAC's method of clustering databases increases scalability (because servers can easily be added or subtracted), lowers costs (because extra high-end servers are not needed), and improves availability (because if a server fails, another can assume its workload).
Radware Load Balancer	Radware Load Balancer
Red Hat	Red Hat provides Linux and open source software.
resolutionState	Event resolution state. Values: NEW,CLOSED
RESTful APIs	See RESTful API Design and Representational State Transfer
Reverse collector	Server-initiated collection procedure typically used when the collector

	cannot initiate a connection because of security considerations.
RFC	Request For Comments
S	
SaaS	Software as a Service
SAP_App_Server_Entry_Point	SAP Application Server
secpol.msc	Local security policy editor
Security Identifier	See SID
ServiceWatch Entry Point	Entry point to the ServiceWatch application
SharePoint connection/portal	URL to the SharePoint site
SID	A Security Identifier is a unique alphanumeric character string assigned by a Windows Domain controller during the log on process. It identifies a user or group of users in a network.
SMTP	Simple Mail Transfer Protocol
Sniffer	A packet analyzer (network analyzer, protocol analyzer, packet sniffer, Ethernet sniffer or wireless sniffer) is software or computer hardware that intercepts and logs traffic passing over a network.
SNMP	Simple Network Management Protocol
Solaris	A Unix operating system originally developed by Sun Microsystems. It is now maintained by Oracle.
SolarWinds	SolarWinds Network Performance Monitor detects, diagnoses and resolves network performance problems and outages.
Splunk Enterprise	Splunk Enterprise converts machine data generated by IT systems and technology infrastructure into information about the status of computer networks and applications running on them.
SQL Server Analysis Services	SQL Server Analysis Services
SQL Server Integration	SQL Server Integration Services
SQL Server Reporting	SQL Server Reporting Services
SSAS	SQL Server Analysis Services
SSIS	SQL Server Integration Services
SSIS File EP	SSIS Execute Package file
SSIS Job	SQL Server Integration Services job
SSRS	SQL Server Reporting Services
Storage Array	Disk Array
Stty command	This command sets or displays terminal/console settings.
sudo	A program for Unix-like operating systems that allows users to run programs with the security privileges of another user (normally the superuser, or root). Its name is a concatenation of `'su'` (substitute

	user) and 'do''do', or take action.
Sun Directory Proxy Server	Sun Directory Proxy Server FAQ
Sun iPlanet Web Server	iPlanet
Sun LDAP Server	Configuring an LDAP Proxy
SUSE	An enterprise Linux distribution.
SWaaS	ServiceWatch as a Service (see Chapter 3: ServiceWatch as a Service)
Sybase	Sybase client-server relational database
Symantec NetBackup OpenStorage	See also Hitachi Storage systems
Symmetrix	EMC Corporation's storage array.
T	
TAM	IBM Tivoli Access Manager is an authentication and authorization solution for corporate web services, operating systems, and existing applications. TAM runs on various OSs such as Unix (AIX, Solaris, HP-UX), Linux, and Microsoft Windows. Like other Tivoli products, it has been renamed as IBM Security Access Manager.
TBS	Technical Business Service: A user-specified collection of CIs whose features or connections make it worthwhile to treat them as a group.
TCP	Transmission Control Protocol
Tibco	Tibco Software
Tibco Active Matrix Business	Tibco ActiveMatrix BusinessWorks
Tibco BW	Tibco BusinessWorks
Tibco BW process	Tibco BW process design guide and concepts
Tibco EMS Queue	Tibco Enterprise Message Service routing design
Tibco Enterprise Message	Tibco Enterprise Message service
Tibco File Listener	Tibco Rendezvous Listener
Tibco Hawk EP	Tool for monitoring and managing distributed applications and OSs
Tivoli Netcool	See Netcool
TNS	Oracle Transparent Network Substrate enables peer-to-peer connectivity where machine-level connectivity cannot occur. It provides a user-transparentlayer that enables a heterogeneous network consisting of different protocols to function as a homogeneous network.
Tomcat	Apache Tomcat
Tomcat WAR	Tomcat Web Archive file
Topology map	In the **Topology Map** screen, ServiceWatch performs a top-down discovery from each entry point defined in the **Entry Point** screen and

	displays a **Topology Map** of the objects in the business service.
U	
Ubuntu	Linux Server operating system. See http://www.ubuntu.com/
uCMDB	HP Universal Configuration Management Database
URL	Uniform Resource Locator
V	
vCenter Server	Virtual Server
Virtual Directory	Virtual Directory
vm uuid	Virtual Machine Universal ID
VMware	Virtual Machine ware
VMware Knowledge Base	The VMware Knowledge Base provides support solutions, error messages, and troubleshooting guides.
vmwVC	vmwVC event codes
VSAM	Virtual storage access method is an IBM DASD file storage access method, first used in the OS/VS1, OS/VS2 Release 1 (SVS) and Release 2 (MVS) operating systems, later used throughout the Multiple Virtual Storage (MVS) architecture and now in z/OS.
W	
Wallet (Oracle)	Oracle wallet: a mechanism for storing and distributing user names and passwords
wbemtest	A utility for testing and exploring WMI. Link1 Link2 Link3 Link4
WebLogic JMS Server	WebLogic JMS Server configuration
WebLogic Module	Plugins for WebLogic Server
WebLogic PS	WebLogic Portal Server
WebSEAL	Multi-threaded Web server that applies fine-grained security policy to a (Tivoli) Access Manager protected Web object space. WebSEAL
WebSphere	IBM's application and integration middleware
WebSphere EAR	WebSphere Enterprise ARchive
WebSphere ODR	WebSphere On-demand router
WebSphere Portal	WebSphere Portal
wget	Wget retrieves content from web servers and is part of the GNU

	Project. Its name is derived from *World Wide Web* and *get*. It downloads via HTTP, HTTPS & FTP protocols
WMB Flow	WebSphere Message Broker: Configuring flows for monitoring video
WMI	Windows Management Instrumentation is Microsoft's implementation of Web-Based Enterprise Management (WBEM), a technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM) standard to represent systems, applications, networks, devices and other components.
wmic	Windows Management Instrumentation Command-line
WS	See WebSphere in this glossary.
X	
Xen	An open source virtualization standard. See also XenServer
XenApp or Presentation Server Components	Presentation Server 4.5 and Components
XenApp or Presentation Server EP	XenApp Execute Package
xjc tool	Java tool for XML binding
Y	
Z	

Appendix D: Adding HTTPS Support

For general information about configuring SSL in a Jetty web server, see
http://wiki.eclipse.org/Jetty/Howto/Configure_SSL

Configuration Steps

Copy neebula.jks to the Custom Directory

If this Java KeyStore file is not copied, it will be deleted by the upgrade.

1. **C:\Neebula\ServiceWatch\server\conf\neebula.jks ==>**
   C:\Neebula\ServiceWatch\server\conf\custom\neebula.jks
2. The KeyStore password is iam100%

Create a key with Java Keytool or import a key into KeyStore

3. This command generates a key pair and certificate directly into a Java Keystore:
   keytool -keystore keystore -alias jetty -genkey -keyalg RSA

   This command generates the file jetty.csr for a key/cert that is already in the Keystore: keytool -certreq -alias jetty -keystore keystore -file jetty.csr

Generating Keys and Certificates with OpenSSL

4. This command generates a key pair in the **jetty.key** file:
   openssl genrsa -des3 -out jetty.key
5. If you have a key and certificate in separate files, combine them into a PKCS12 format file to load
   into a new KeyStore. The certificate can be one you generate yourself *or* one returned from a CA
   (Certification Authority) in response to your CSR (Certificate Signing Request).

   This OpenSSL command combines the keys in jetty.key and the certificate in the jetty.crt file into the jetty.pkcs12 file:
   ```
   openssl pkcs12 -inkey jetty.key -in jetty.crt -export -out
   jetty.pkcs12
   ```

   Or you can use Java Keytool (version jdk1.6 or later) to import a PKCS12 file with this command:
   ```
   keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype
   PKCS12
   -destkeystore keystore
   ```

Create a CSR and send it to the Certification Authority

Generate a CSR with keytool

6. This command uses Keytool to generate the **jetty.csr** file for a key and certificate that exist in the KeyStore:

```
keytool -certreq -alias jetty -keystore keystore -file jetty.csr
```

Or generate a CSR with OpenSSL

This command uses OpenSSL to generate a **jetty.csr** file for a key that exists in the **jetty.key** file:

```
openssl req -new -key jetty.key -out jetty.csr
```

Loading Certificates with Java Keytool

Encrypted PEM format certificates are produced by OpenSSL and returned by some CAs.

You can use Java Keytool to load an encrypted PEM format certificate directly into a KeyStore.

jetty.crt is an example of a PEM format certificate.

```
-----BEGIN CERTIFICATE-----
MIICSDCCAfKgAwIBAgIBADANBgkqhkiG9w0BAQQFADBUMSYwJAYDVQQKEx1Nb3J0
IEJheSBDb25zdWx0aW5nIFB0eS4gTHRkLjEOMAwGA1UECxMFSmV0dHkxGjAYBgNV
BAMTEWpldHR5Lm1vcnRiYXkub3JnMB4XDTAzMDQwNjEzMTk1MFoXDTAzMDUwNjEz
MTk1MFowVDEmMCQGA1UEChMdTW9ydCBCYXkgQ29uc3VsdGluZyBQdHkuIEx0ZC4x
DjAMBgNVBAsTBUpldHR5MRowGAYDVQQDExFqZXR0eS5tb3J0YmF5Lm9yZzBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQC5V4oZeVdhdhHqa9L2/ZnKySPWUqqy81riNfAJ
7uALW0kEv/LtlG34dOOcVVt/PK8/bU4dlolnJx1SpiMZbKsFAgMBAAGjga4wgasw
HQYDVR0OBBYEFFV1gbB1XRvUx1UofmifQJS/MCYwMHwGA1UdIwR1MHOAFFV1gbB1
XRvUx1UofmifQJS/MCYwoVikVjBUMSYwJAYDVQQKEx1Nb3J0IEJheSBDb25zdWx0
aW5nIFB0eS4gTHRkLjEOMAwGA1UECxMFSmV0dHkxGjAYBgNVBAMTEWpldHR5Lm1v
cnRiYXkub3JnggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADQQA6NkaV
OtXzP4ayzBcgK/qSCmF44jdcARmrXhiXUcXzjxsLjSJeYPJojhUdC2LQKy+p4ki8
Rcz6oCRvCGCe5kDB
-----END CERTIFICATE-----
```

7. This command imports the PEM format certificate from the `jetty.crt` file to a JSSE

(64-bit Secure Socket Extension) KeyStore:

```
keytool -keystore
C:\Neebula\ServiceWatch\server\conf\custom\neebula.jks
-import -alias jetty –file jetty.crt –trustcacerts
```

If you do *not* require the **`-trustcacerts`** option, try the command without it.

8. This command imports a CA certificate:

keytool -**`import`** -trustcacerts -alias root -file Thawte.crt -keystore keystore.jks

9. If the certificate you receive from the CA is not in a format that Keytool understands, use the

`openssl` command to convert formats:

```
openssl x509 -in jetty.der -inform DER -outform PEM -out jetty.crt
```

10. Delete the ServiceWatch OOTB (out of the box) certificate with this command:

```
keytool -keystore neebula.jks -delete -alias servercert
```

11. You can use this command to list keystore contents:

```
keytool -keystore neebula.jks -list
```

To change the HTTPS port from 8443 to 443 & disable the HTP port

Edit the server\conf\jetty properties:

```
# enable http
# http.port=8080

# enable https
https.port=443
```

and on each collector, edit the conf\custom\activeprobe-client.properties

```
com.neebula.orchestrator.collector.activeprobe.port=443
```

Appendix E: ServiceNow CMDB Integration

Introduction

ServiceWatch uses a unique 'top-down' discovery method to map the business service and all of its associated CIs. The integration retrieves business service data from ServiceWatch, translates the retrieved data to ServiceNow CI types, and populates the relationships in ServiceNow CMDB. The integration also creates a view of the business service itself so an accurate topology map can be accessed within ServiceNow.

This document describes the integration architecture and explains how to configure and tailor the integration for your ServiceNow CMDB implementation.

CMDB Integration Connector

The integration can run in either a local environment or in a cloud environment. A 3rd party connector between ServiceWatch and ServiceNow enables the synchronization of the ServiceWatch CMDB information with the ServiceNow CMDB. This connector requires HTTPS connectivity.

Note: Only a single **Connector for ServiceNow** can be used for the CMDB integration. If two or more connectors are created, the exported changes will not be consistent.

Export Types

Data is exported from the ServiceWatch CMDB to the ServiceNow CMDB over the configured connector. This mechanism enables topology changes detected by the ServiceWatch 'Rediscovery' process to be transferred to ServiceNow as often as required.

Two types of data export are performed – Incremental and Full:

1. During full export, all the CMDB data of ServiceWatch is exported to ServiceNow. This export takes place when the connector is established and, after that, once every N incremental exports, according to the specified configuration.
2. Incremental exports include only those changes that occur after the last full export. The rate of incremental exports is configurable (once every M minutes). Exported changes include Business Service activation/de-activation, addition/removal of CIs, and addition/deletion of connections.

Effects of Exported Changes in ServiceNow

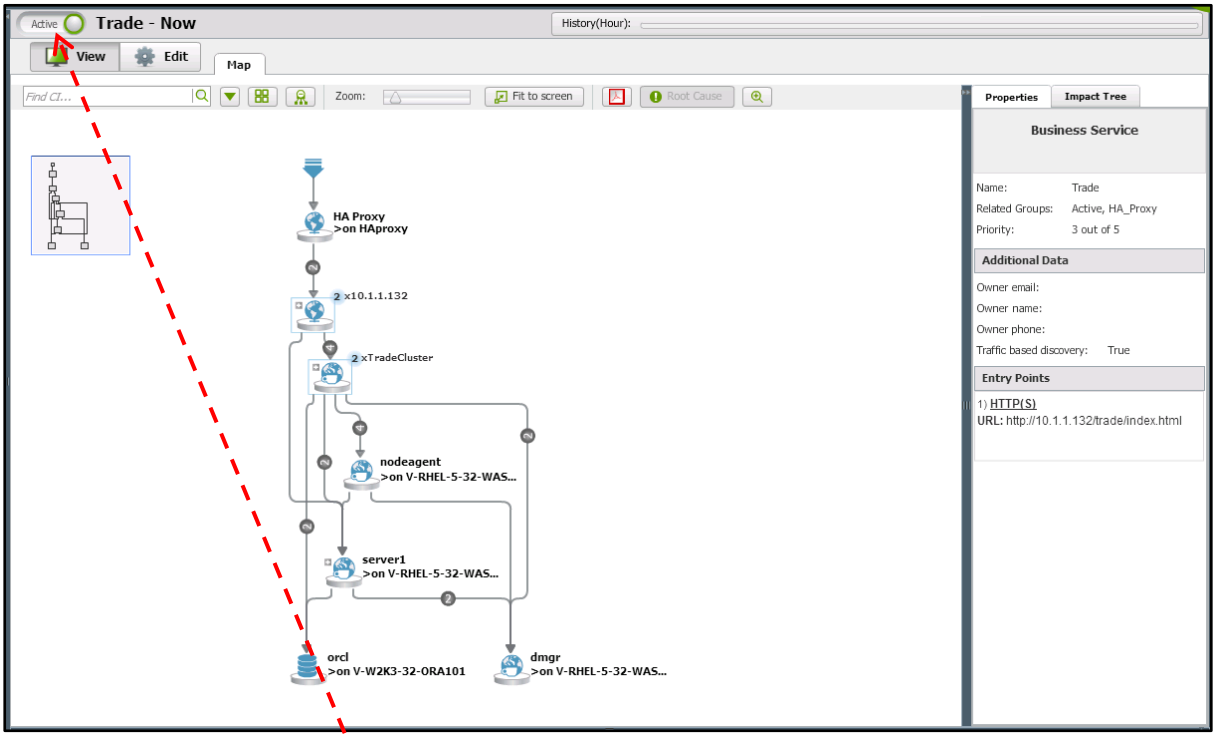
As a result of the exported changes in ServiceWatch, the following changes occur at the ServiceNow CMDB:

a. Business services that were activated in ServiceWatch (see Figure 249) are created in ServiceNow (see Figure 251).

b. Business services that were deactivated in ServiceWatch (see Figure 250) are deleted from ServiceNow.

Note: When a business service is deactivated, it is removed from the ServiceNow CMDB but its CIs and relations are not removed. When a business service is activated, it is recreated in the ServiceNow CMDB.

Figure 249: Example of a Business Service that is active in ServiceWatch



Note: Toggle the Inactive / Active button to activate / deactivate the Business Service.

Figure 250: Example of a Business Service that is *not* active in ServiceWatch

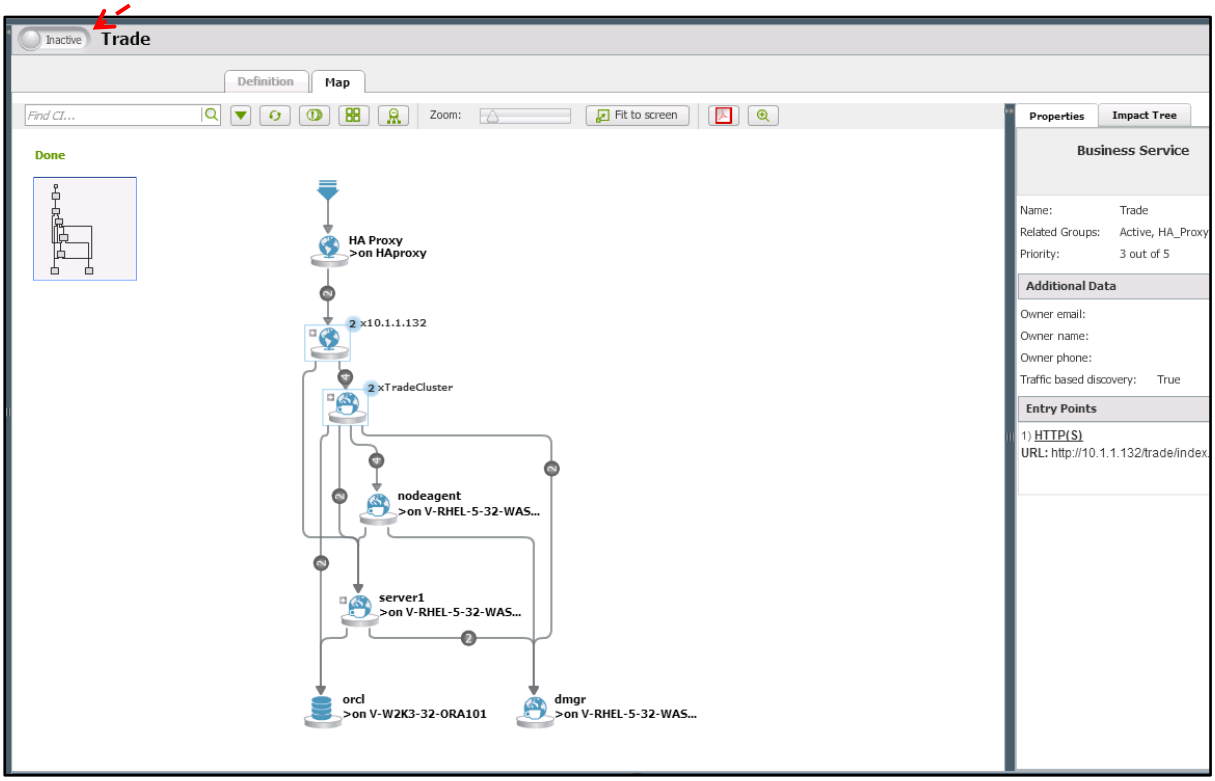
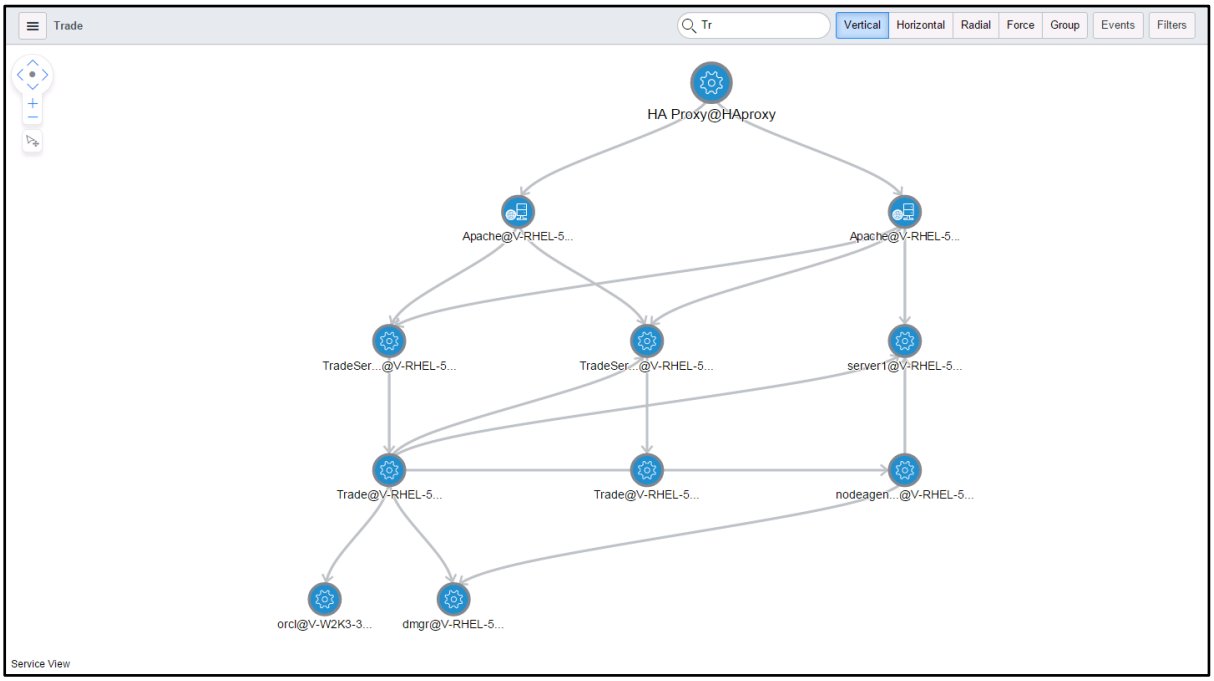


Figure 251: Example of a Business Service in ServiceNow



c. CIs that were added to a business service in ServiceWatch are added to that business service in ServiceNow.

d. CIs that were removed from a business service in ServiceWatch are removed from that business service in ServiceNow.

e. Connections that were added to a business service in ServiceWatch are added to that business service in ServiceNow.

f. Connections that were deleted from a business service in ServiceWatch are deleted from a that business service in ServiceNow

Configuring the Connector for ServiceNow

The 3rd party **Connector for ServiceNow** must be defined in ServiceWatch. The dialog box that defines this connector is illustrated and described in Figure 110 and also shown below.

This dialog box is reached via the Menu item: **Settings > System > Monitoring connectors**.

Click the **+** in the upper right corner and select **connector for ServiceNow**.

The connector's configuration includes the following parameters:

- Frequency (minutes)
- Full export every Nth time

  Note: You can set the frequency in which incremental exports will occur. A 'Full' export occurs every N^{th} incremental export.

- URL of the ServiceNow instance

  For example, **`https:// Instance_name.service-now.com`**

- Username & password for the ServiceNow instance

Optional parameters:

- Description
- Create Hosts

  If this checkbox is selected, hosts detected by ServiceWatch are transferred to ServiceNow. The information is then merged with the hosts detected by ServiceNow.

  Note: A Load Balancer discovered by ServiceWatch is displayed with its host in ServiceNow even if the **Create Hosts** checkbox is *not* selected.

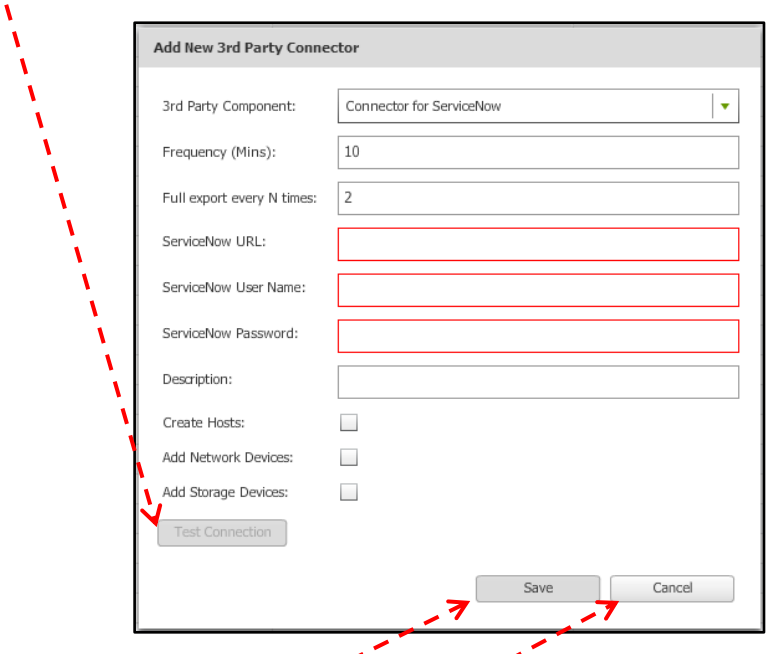
- Add Network Devices

  If this checkbox is selected, Network devices detected by ServiceWatch are transferred to ServiceNow.

- Add Storage Devices

  If this checkbox is selected, Storage devices detected by ServiceWatch are transferred to ServiceNow.

  You can test the connection before saving the configuration by clicking the **Test Connection** button.



The configuration can be saved or canceled by pressing the appropriate button.

Tailoring the Integration

Mapping ServiceWatch-Discovered CIs to ServiceNow CIs

ServiceWatch-discovered CIs are translated to ServiceNow CI format. The transformation results in CIs which are identical to ServiceNow-discovered components. This CI-to-CI mapping is configurable via a metadata configuration file (**sn-mapping.xml**) that allows any type of ServiceWatch-discovered CIs, attributes and relationships to be translated and imported to ServiceNow CMDB objects.

The integration supports all CI types and Entry Point types defined in ServiceWatch.

By default, if not otherwise specified, CI or Entry Point types are mapped to the Generic ServiceNow CI.

You can extend support for new CIs by using the metadata configuration file **sn-mapping.xml** as explained below.

Web Services

After the data is converted to ServiceNow format, the integration accesses ServiceNow using the ServiceNow Web Services API described in the SERVICENOW PRODUCT DOCUMENTATION website.

The integration uses the following processes to populate ServiceNow CMDB objects:

- ServiceWatch CIs that are part of a business service are identified and marked as that business service's members.
- The integration checks the relationships in ServiceNow between each CI and its business service. If a ServiceWatch-discovered application flow indicates a change is needed, the relationship is updated and any missing CIs are added to the ServiceNow CMDB.

sn-mapping.xml File

The **sn-mapping.xml** file is used to map ServiceWatch CIs and attributes to ServiceNow CIs and attributes. New CIs can be supported by modifying the file.

Sample sn-mapping.xml file

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-3.0.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.springframework.org/schema/beans">
<!-- CIT Mapping Rules Available Neebula CI attributes to use for CMDB attributes
population/transformation: id version label description typeName bsId bsName
host.Short_host_name - short representation of host name (not fqdn)
host.serial_number host.primary_management_ip host.primary_host_name - fqdn
host.primary_host_name_or_ip host.os_type - operating system name (for example
WINDOWS_2008) host.oS_family - operating system name (for example WINDOWS)
host.os_version host.model host.domain host.address_width type - represents the
```

```
connection type (HTTP, TCP, etc...) *application specific attributes per Neebula
CIT are also available (for example instance in all data base servers) -->
<!-- #This is an example bean <bean id="cmdb_ci_app_server_websphere"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping">
#cmdbCIT represents the name of the CI type on CMDB side <property name="cmdbCIT"
value="cmdb_ci_app_server_websphere"/> #neebulaCIT represents the name of the CI
type on Neebula side, you can place mutiple CIT with , as delimiter between them
<property name="neebulaCIT" value="Websphere"/> #mappingRules contain a list of
mapping rules which populate the CMDB CIT attributes. #The key represents the CMDB
attribute name and the value should contain an expression that should define the
desired value. #The expression may contain the next operators/operands: #+ for
concatenation #${attName} - represents an attribute value: for example ${version}
will return the value of the the version attribute on Neebula CI #'' - for constant
values #Additional transformation capabilities can be looked at
http://groovy.codehaus.org/User+Guide <property name="mappingRules"> <map key-
type="java.lang.String" value-type="java.lang.String"> <entry
key="install_directory" value="${install_dir}"/> <entry key="server_root"
value="${server_root}"/> <entry key="config_directory" value="${conf_dir}"/> <entry
key="cell" value="${cell}"/> <entry key="node" value="${node}"/> <entry key="name"
value="${server}+'@'+${host.primary_host_name_or_ip}"/> <entry key="version"
value="${version}"/> <entry key="location" value="${location}"/> <entry
key="sys_class_name" value="'cmdb_ci_app_server_websphere'"/> <entry
key="ip_address" value="${host.primary_management_ip}"/> </map> </property>
#KeyRules contain a list of matching rules that are used to locate a specific
instance on the CMDB side. #It is basically the integration identity matching rules
for this specific CIT. #The list contains 2 maps - Between each entry in a map,
there is an AND relationship - i.e. all these attributes must match #in order to
determine that 2 cis in ServiceNow are matching. #Between the 2 maps there is an OR
relationship - i.e. If the first set of entries doesn't match, #then the second set
of entries tries to match <property name="keyRules"> <list> <map key-
type="java.lang.String" value-type="java.lang.String"> <entry key="cell"
value="${cell}"/> <entry key="node" value="${node}"/> <entry key="name"
value="${server}+'@'+${host.primary_host_name}"/> </map> <map key-
type="java.lang.String" value-type="java.lang.String"> <entry key="cell"
value="${cell}"/> <entry key="node" value="${node}"/> <entry key="name"
value="${server}+'@'+${host.primary_management_ip}"/> </map> <map key-
type="java.lang.String" value-type="java.lang.String"> <entry key="name"
value="${server}+'@'+${host.primary_host_name}"/> </map> <map key-
type="java.lang.String" value-type="java.lang.String"> <entry key="name"
value="${server}+'@'+${host.primary_management_ip}"/> </map> </list> </property>
</bean> -->
<!-- ======================== APP_DOMAIN ======================== -->
```

< long snip >

```
bean="fallback_match_by_hostname"/><ref
bean="fallback_match_by_ip"/></list></property></bean><bean
class="com.neebula.orchestrator.processing.integration.cmdb.CMDBToNeebulaMapping"
id="cmdb_ci_appl_cisco_fibre"><property value="cmdb_ci_appl_cisco_fibre"
name="cmdbCIT"/><property value="Cisco Fibre InterConnect"
name="neebulaCIT"/><property name="mappingRules"><map value-type="java.lang.String"
key-type="java.lang.String"><entry value="${serial}" key="serial_number"/><entry
value="${model}" key="model_number"/><entry value="${dn}"
key="distinguished_name"/><entry value="${location}" key="location"/><entry
value="'cmdb_ci_appl_cisco_fibre'" key="sys_class_name"/><entry
value="${host.primary_management_ip}" key="ip_address"/><entry
value="${label}+'@'+${host.primary_host_name_or_ip}"
key="name"/></map></property><property name="keyRules"><list><map value-
type="java.lang.String" key-type="java.lang.String"><entry value="${dn}"
key="distinguished_name"/><entry value="${label}+'@'+${host.primary_host_name}"
key="name"/></map><map value-type="java.lang.String" key-
type="java.lang.String"><entry value="${dn}" key="distinguished_name"/><entry
value="${label}+'@'+${host.primary_management_ip}" key="name"/></map><ref
bean="fallback_match_by_hostname"/><ref
bean="fallback_match_by_ip"/></list></property></bean></beans>
```

Modifying the mapping.xml File

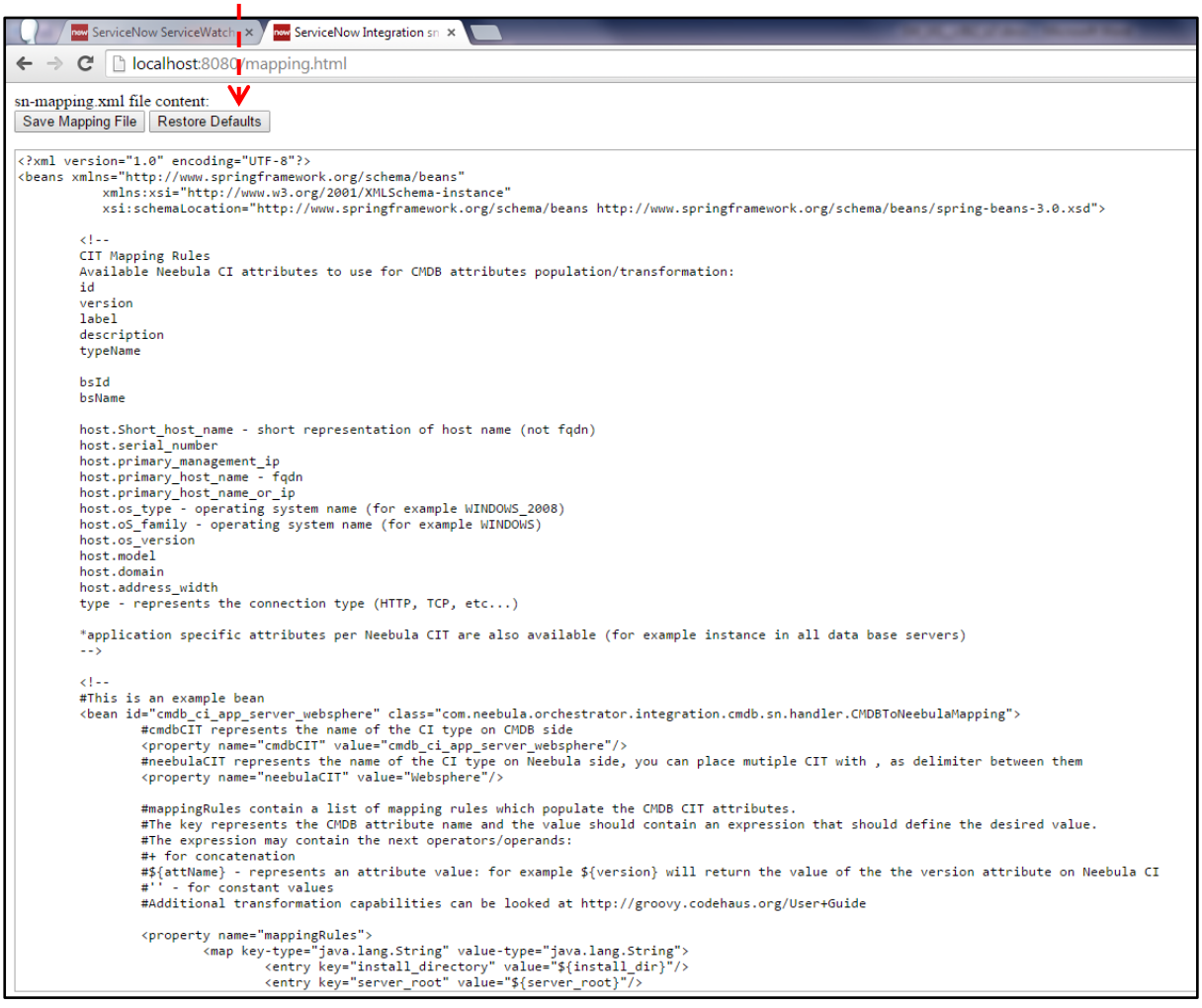
To modify this file:

1. Use your browser to access **`localhost:8080/mapping.html`**
   The **mapping.xml** file will be displayed in the editor.
2. Implement the desired changes.
3. Save changes by clicking the Save Mapping File button.

Restore Defaults Button

The Restore Defaults button restores the factory default values that were set when ServiceWatch was first installed. Values that were added after the installation will not be part of the 'Restore Defaults'.

Figure 252: Integration screen (with sn-mapping.xml file and Restore Defaults button)



CI conversion – attributes

CIs binding and conversion is based on the CI's attributes. Any ServiceWatch attribute that is available for a CI (as defined in the CI-Type definition) can be used in the conversion and binding procedures.

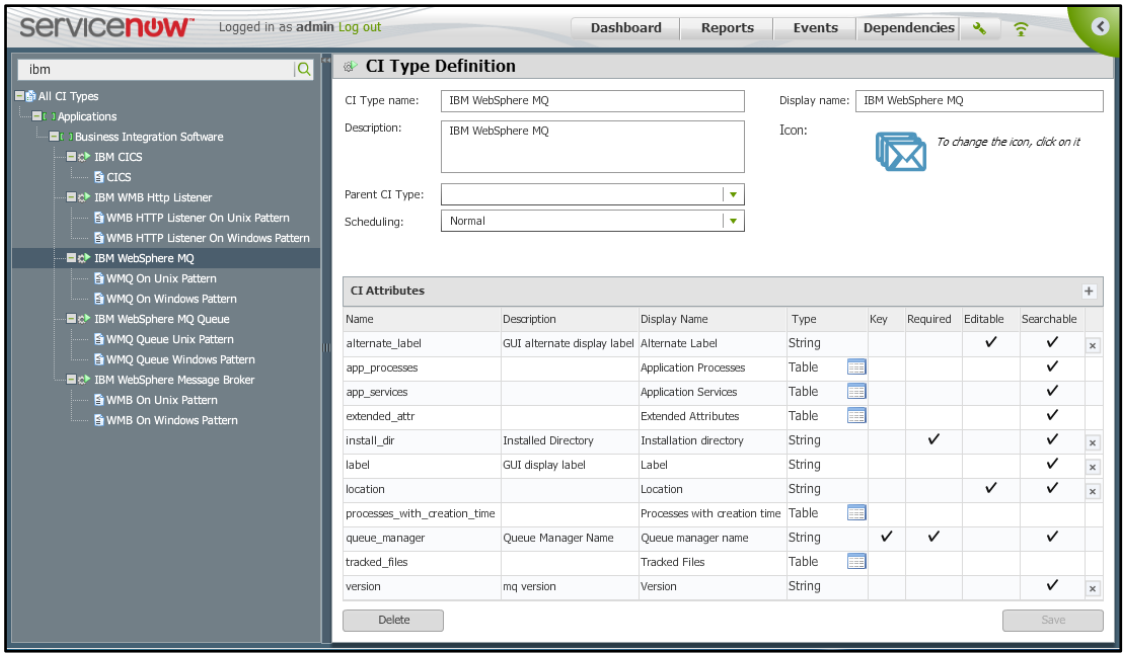
The following attributes are automatically populated and available for conversion for each ServiceWatch CI.

Note: The attribute name below is the name that should be used in the definition:

Attribute	Description
Id	**ServiceWatch CI ID number – used to create an attribute inside ServiceNow for a change impact analysis launch in context URL in ServiceWatch. Example:** `http://(neebula)/ui/?screen=physical&ciid=8763)`
host.Short_host_name	**Short representation of host name (not fqdn)**
host.Serial_number	**Serial number of the host on which the CI is resident; functions as primary key for host binding**
host.Primary_management_IP	
host.Primary_host_name fqdn	**Fully qualified domain name or IP**
host.OS_Type	**operating system name**
host.OS_Version	**Includes the patch level of the OS**
host.Model	
host.Domain	
host.Address_Width	

All other CI type attributes (as defined in the ServiceWatch CI) are available for conversion. E.g. an IBM WebSphere MQ ServiceWatch attributes:

Figure 253: Example of a ServiceWatch CI's attributes



CI Attribute Translation - Example

```
<bean id="cmdb_ci_app_server_websphere" class=
"com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping ">
      <property name="cmdbCIT" value="cmdb_ci_app_server_websphere"/>
      #neebulaCIT represents the name of the CI type on Neebula side, you can
      place multiple CIs with "," as a delimiter between them
      <property name="neebulaCIT" value="Websphere"/>
      <property name="mappingRules">
            <map key-type="java.lang.String" value-type="java.lang.String">
                  <entry key="install_directory" value="${install_dir}"/>
                  <entry key="server_root" value="${server_root}"/>
                  <entry key="config_directory" value="${conf_dir}"/>
                  <entry key="cell" value="${cell}"/>
                  <entry key="node" value="${node}"/>
                  <entry key="name"
                  value="${server}+"@"+${host.primary_host_name_or_ip}"/>
                  <entry key="version" value="${version}"/>
                  <entry key="location" value="${location}"/>
                  <entry key="sys_class_name"
      value=""cmdb_ci_app_server_websphere""/>
                  <entry key="ip_address" value="${host.primary_management_ip}"/>
="keyRules">
            <list>
                  <map key-type="java.lang.String" value-type="java.lang.String">
                        <entry key="cell" value="${cell}"/>
                        <entry key="node" value="${node}"/>
                        <entry key="name"
value="${server}+"@"+${host.primary_host_name}"/>
                  </map>
                  <map key-type="java.lang.String" value-type="java.lang.String">
                        <entry key="cell" value="${cell}"/>
                        <entry key="node" value="${node}"/>
                        <entry key="name"
value="${server}+"@"+${host.primary_management_ip}"/>
                  </map>
                  <map key-type="java.lang.String" value-type="java.lang.String">
                        <entry key="name"
value="${server}+"@"+${host.primary_host_name}"/>
                  </map>
                  <map key-type="java.lang.String" value-type="java.lang.String">
                        <entry key="name"
value="${server}+"@"+${host.primary_management_ip}"/>
                  </map>
            </list>
      </property>
</bean>
```

Example CI-to-CI mapping

Text in the File	Explanation
<property name="cmdbCIT" value= "cmdb_ci_app_server_websphere"/>	Name of the ServiceNow CI Type
<property name="neebulaCIT" value= "Websphere"/>	Name of the ServiceWatch CI Type. This could also contain a list of CI Types separated by commas
<property name="mappingRules">	Start of the attribute mapping session
<map key-type="java.lang.String" value-type="java.lang.String">String	Type of mapping; in this case String <->
<entry key="Version" value= "${version}"/>	entry key= Name of ServiceNow attribute value= An expression that accepts ServiceWatch attributes in the format ${neebula-CI-att}; ${version} is used in this example. Implanted constants and concatenated variables similar to this example can also be used: value="${label}+"@"+${Primary_host_name}" This example creates a value of Websphere1@mainhost.mycompany.local Very complex translations can be created with appropriate code. For more information see http://groovy.codehaus.org/User+Guide
<property name="keyRules">	Defines how to create a CI Key in ServiceNow and the order in which keys are compared for CI binding in ServiceNow. The comparison order is predefined.

Common attributes

This section specifies common attributes that are automatically added to all exported CIs and connections:

```
<!-- defines common attributes values that will be set on each update/insert action-->
<bean id="common_attributes_values" class="java.util.HashMap">
        <constructor-arg index="0" type="java.util.Map">
                <map key-type="java.lang.String" value-type="java.lang.String">
                        <entry key="discovery_source" value="ServiceWatch"/
                </map>
        </constructor-arg>
</bean>
```

This section specifies common attributes that are automatically added to exported CIs:

```
<!-- defines common attributes values for ci types only that will be set on each update/insert action-->
<bean id="cit_common_attributes_values" class="java.util.HashMap">
        <constructor-arg index="0" type="java.util.Map">
                <map key-type="java.lang.String" value-type="java.lang.String">
                        <entry key="short_description" value="${description}"/>
                        <entry key="operational_status" value="1"/>
                        <entry key="correlation_id" value="${id}"/>
                </map>
        </constructor-arg>
</bean>
```

Connection XML mapping example

```
<bean id="cmdb_ci_endpoint_http"
class="com.neebula.orchestrator.processing.integration.cmdb.CMDBToNeebulaMapping">
        <property name="cmdbCIT" value="cmdb_ci_endpoint_http"/>
        <property name="neebulaCIT" value="HTTP(S)"/>
        <property name="mappingRules">
            <map key-type="java.lang.String" value-type="java.lang.String">
                <entry key="name" value="${url}"/>
                <entry key="host_name" value="${hostname}"/>
                <entry key="ip_address" value="${ip}"/>
                <entry key="port" value="${port}"/>
                <entry key="protocol" value="${protocol}"/>
                <entry key="url" value="${url}"/>
                <entry key="sys_class_name" value="cmdb_ci_endpoint_http"/>
                <entry key="parent" value="${src.id}"/>
                <entry key="child" value="${target.id}"/>
            </map>
        </property>
        <property name="keyRules">
            <list>
                <map key-type="java.lang.String" value-type="java.lang.String">
                    <entry key="name" value="${url}"/>
                    <entry key="host_name" value="${hostname}"/>
                    <entry key="ip_address" value="${ip}"/>
                    <entry key="port" value="${port}"/>
                    <entry key="protocol" value="${protocol}"/>
                    <entry key="url" value="${url}"/>
                    <entry key="sys_class_name" value=""cmdb_ci_endpoint_http""/>
                    <entry key="child" value="${target.id}"/>
                </map>
            </list>
        </property>
 </bean>
```

Relationship XML mapping example

The structure of connections and CIs are mapped the same way using cmdbCIT, neebulaCIT, mappingRules and keyRules.

mappingRules consist of all the parameters of the connection, i.e., the parameters of the entry point type plus two additional parameters: **parent** (mapped to **src.id**) and **child** (mapped to **target.id**). These parameters represent both ends of the connection.

keyRules are the same as the **mappingRules** except **parent** mapping does not exist.

Mapping of Hosts, Network paths and Storage paths

Exporting Hosts, Storage devices and Network gear discovered by ServiceWatch to ServiceNow is configurable. See Monitoring Connectors.

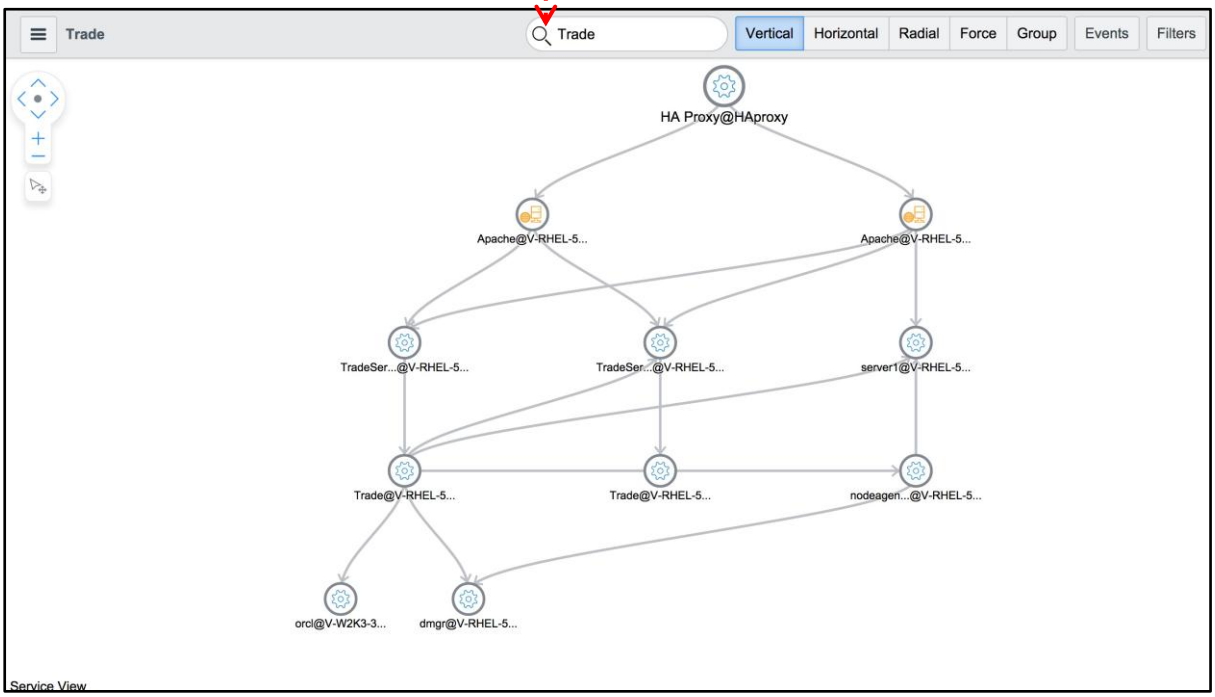
Note: On ServiceNow BSM maps:

- Network and storage devices are displayed as directly connected to the business service CI.
- Hosts are displayed as directly connected to the application CI that runs on that host.

Viewing ServiceWatch's discovered Service in ServiceNow

To display the entire business service, search for its name in the 'Service View' of the ServiceNow BSM Map.

Figure 254: Service View of the ServiceNow BSM Map (Vertical mode)



To display a CI, search for that CI's name in the 'Configuration Items' screen.

Figure 255: Searching for 'HA Proxy' in the ServiceNow Configuration Items screen

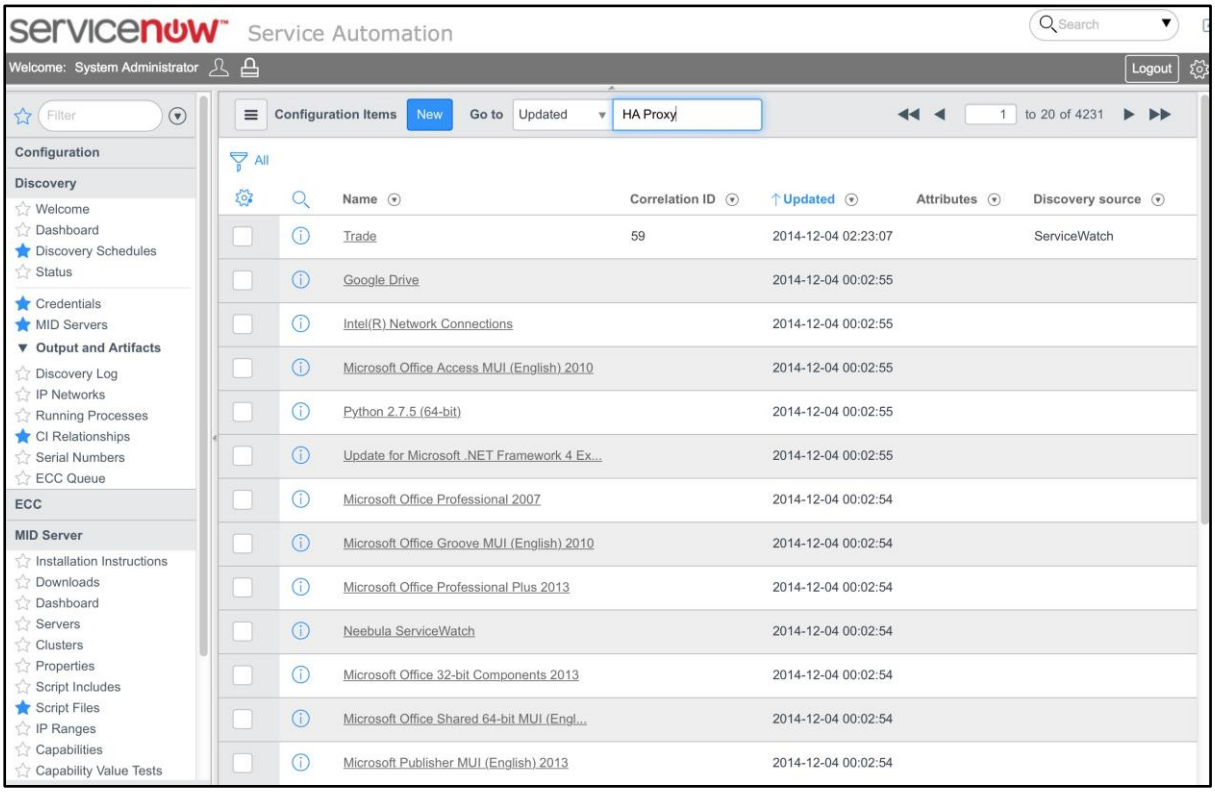


Figure 256: Result of the search for 'HA Proxy'

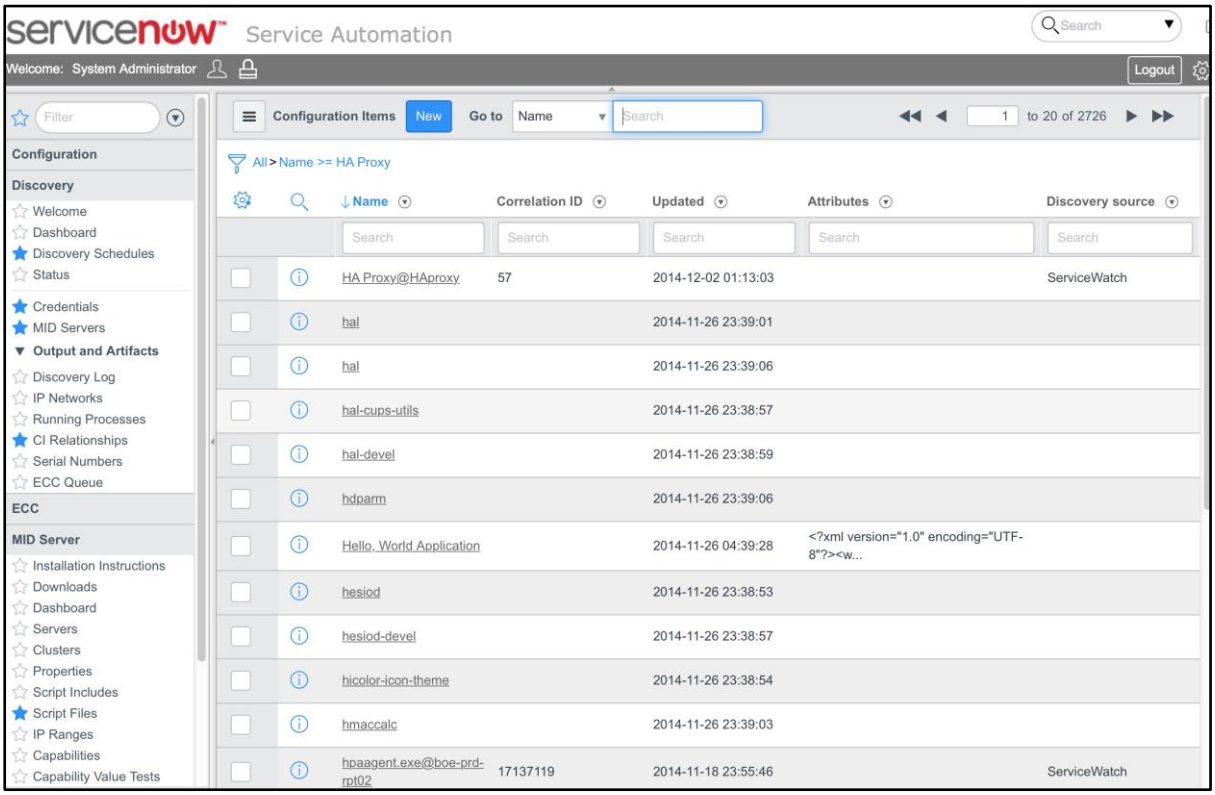


Figure 257: Result of clicking the ⓘ icon in the 'HA Proxy@HAproxy record

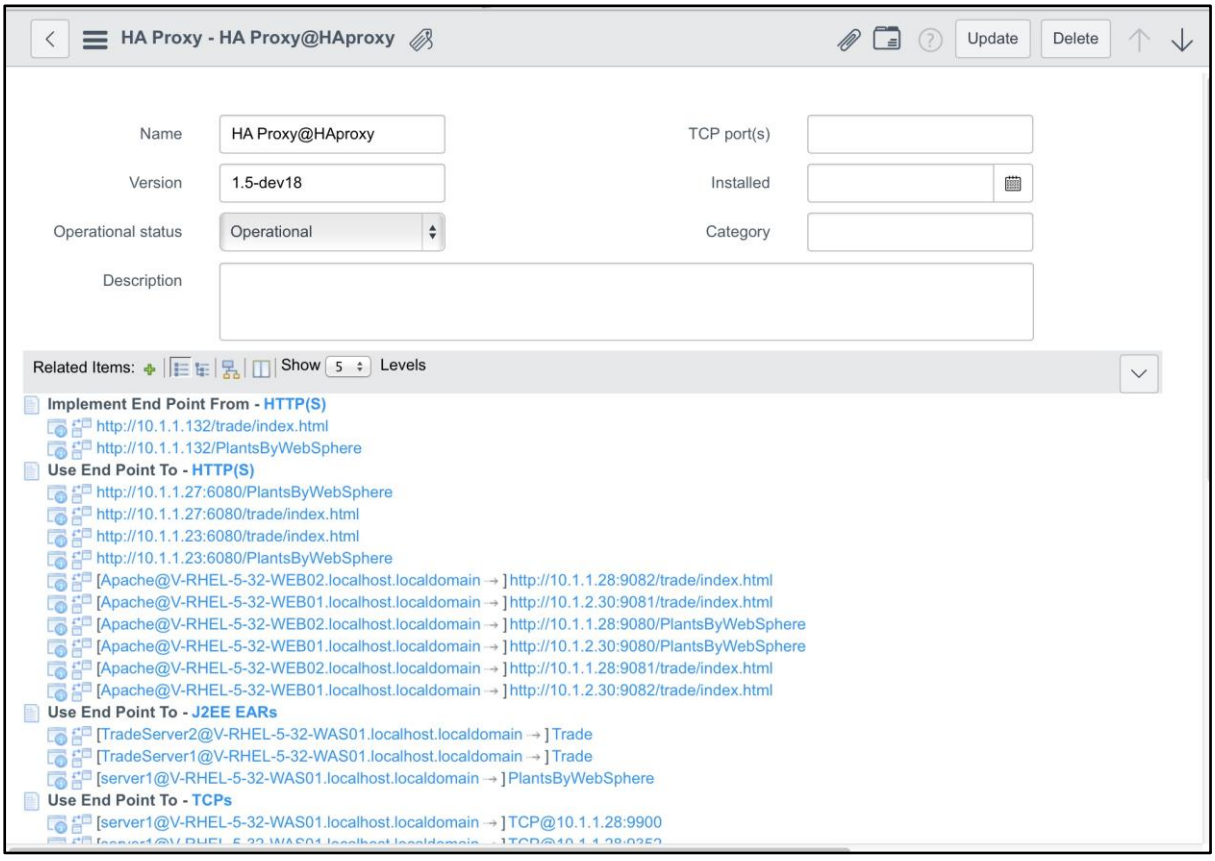
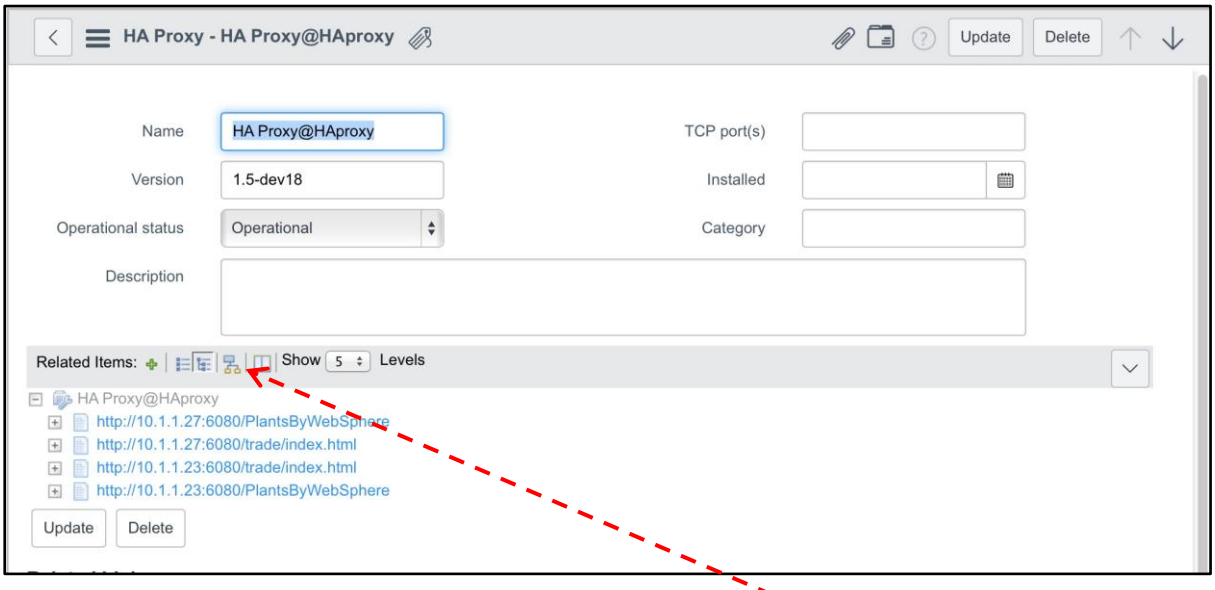
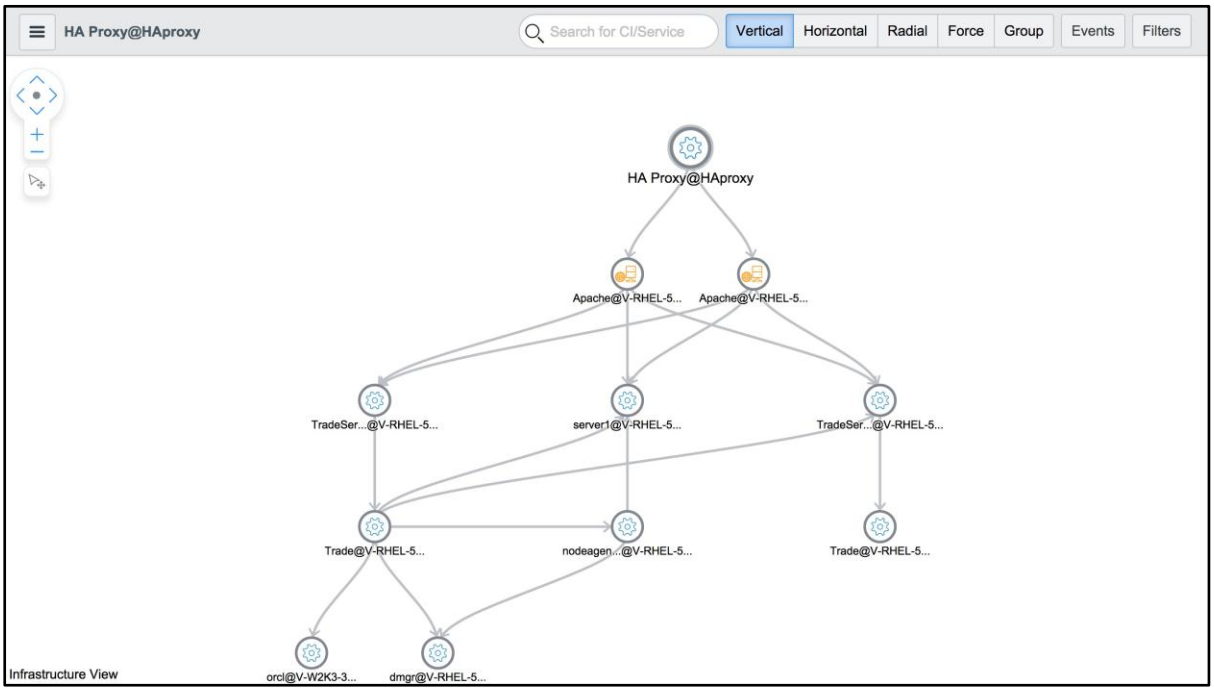


Figure 258: Continuation of the screen in Figure 257



To obtain the Topology Map shown in Figure 259, click the icon (the 4th of the 5 icons after **Related Items)** in the screen shown in Figure 258.

Figure 259: Topology Map (Vertical mode) of HA Proxy@HAproxy



Integration Log files

Information about the last full export is logged in *ServiceWatch's* **cmdb_integration log file.**

To display this log file, go to the **3rd Party Connectors** panel of the **System Health** screen and click the log icon near the right edge of table row for the connector that enables the synchronization of the ServiceWatch CMDB information with the ServiceNow CMDB.

Figure 260: System Health screen – 3rd Party Connectors panel

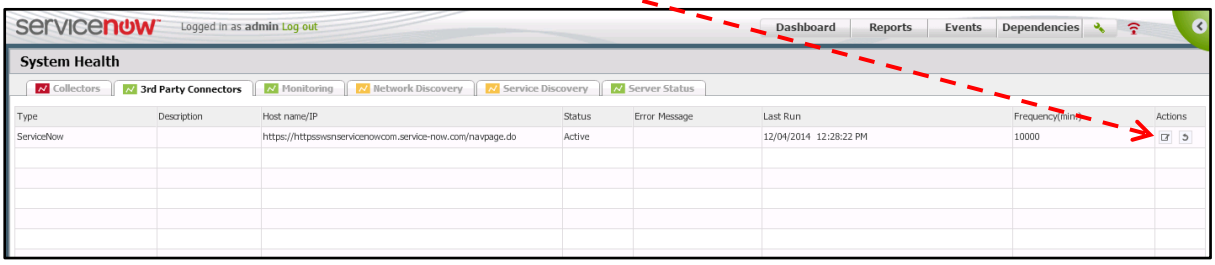
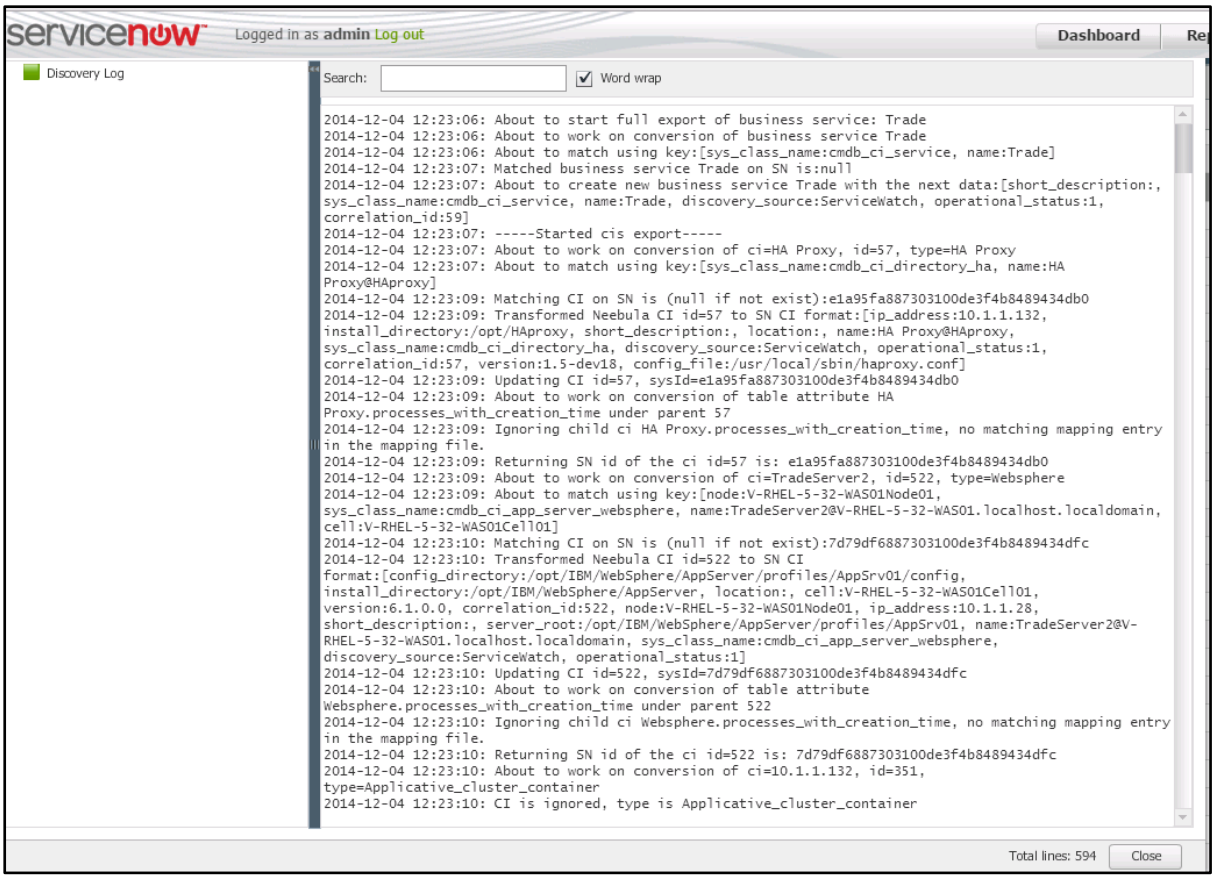


Figure 261: Discovery Log file



Appendix F: ServiceNow Event Integration

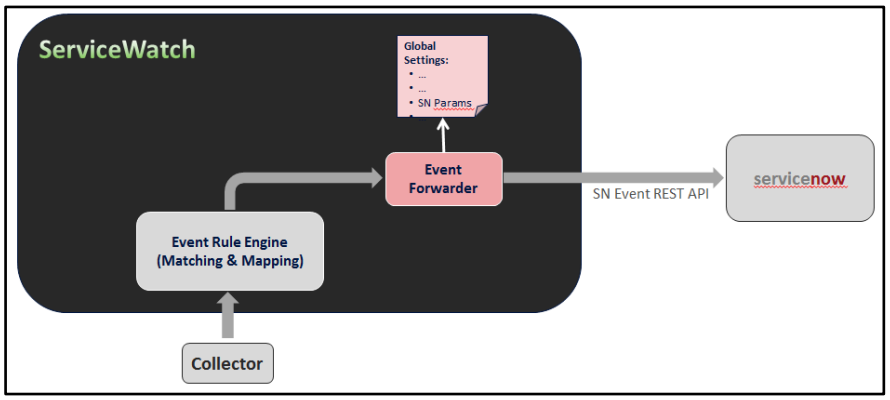
Introduction

When both ServiceWatch and ServiceNow are installed, it may be preferred that events be detected by ServiceWatch in order to monitor event data via ServiceWatch dashboards. Event data detected by ServiceWatch can be forwarded to ServiceNow. This enables ServiceNow to process and handle this event data as if ServiceNow had detected it.

Forwarding Event Data to ServiceNow

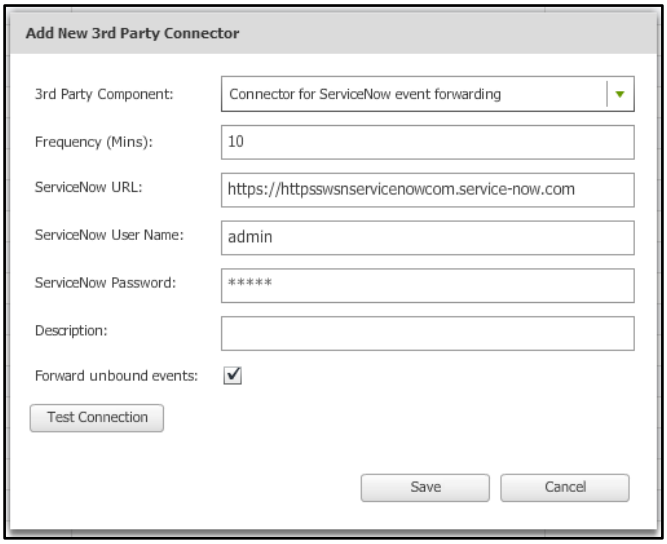
The ServiceWatch server receives event data from several sources. It uses an Event Rule Engine to normalize these events. The integration with ServiceNow enables ServiceWatch to send these normalized events to ServiceNow. The Event Forwarding connector uses a ServiceNow Event REST API for this transfer.

Figure 262: Event Forwarding Flow Diagrsm



Configuring the ServiceNow Event Forwarding Connector

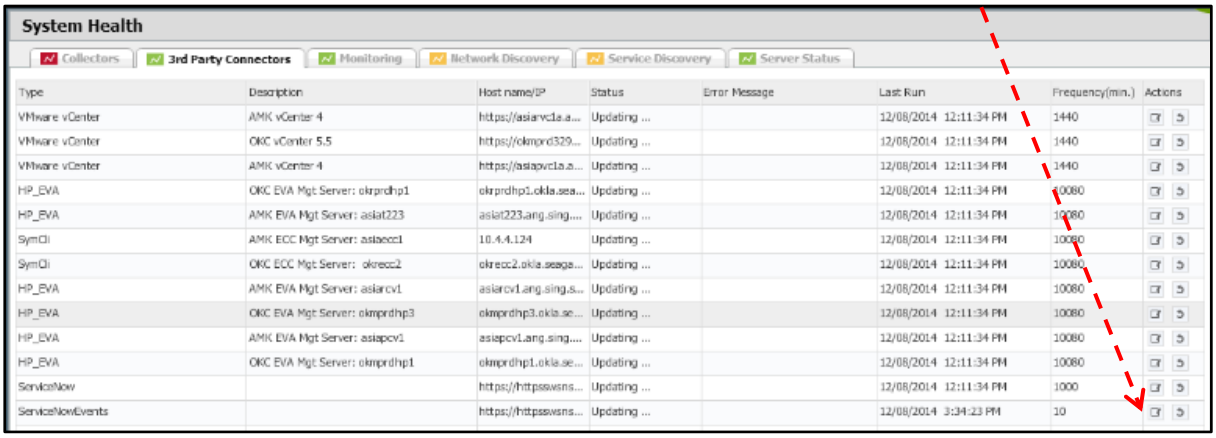
To enable ServiceWatch to send event data to ServiceNow, the **Connector for ServiceNow event forwarding** must be defined and configured. Select **Settings > Monitoring connectors > Connector for ServiceNow event forwarding**. **The Add New 3rd Party Connector** dialog box that defines this connector is illustrated and described in Figure 110 and shown below.



Monitoring the Event Forwarding connector

To display the log file entries for the Event Forwarding connector, go to the **3rd Party Connectors** panel of the **System Health** screen and click the log icon near the right edge of table row for the connector that enables the forwarding of events detected by ServiceWatch to ServiceNow.

Figure 263: System Health screen – 3rd Party Connectors panel



In addition, values for the parameters displayed by the **SN Params** option of the **Settings** menu (see Figure 64) must be specified and a **ServiceWatch Event Forwarder** module must exist in the system.

Mapping / Converting ServiceWatch events to ServiceNow

The following new fields in the **Events** table are used by the event processor to support event normalization and event correlation steps.

ServiceNow Field	ServiceWatch Field	Description or Comment
message_key	messageKey	Unique identifier of an incident. Use the same messageKey in order to override previous event severity
resolution_state	resolutionState	Event resolution state (default: NEW). CLOSING should close the alert (like 'cleared' events)
event_class	emsSystem	Classification of the event (trap, enterprise, syslog, netcool, hpom, etc.)

See Displaying Events on page 164 and Displaying the details of an event in the Unbound Events Table on page 180.

Note: The name of the Event integration connector must be in the form:
https://<instance_name>.service-now.com

It should NOT be of the following form:
https://<instance_name>.service-now.com/navpage.do

Conclusion

We hope the information in this document answers most of your questions about how to implement and run the integration. The ServiceWatch Operations Center staff are ready to provide assistance if required. The ServiceWatch team wishes you success in transferring our accurate up-to-date business service models from ServiceWatch into ServiceNow CMDB.

About ServiceWatch: 'It all Starts with the Map'

ServiceWatch provides Service-Centric Mapping software that improves IT performance and availability through an automated and unified approach to mapping business services which is about 20 times faster and 80 percent less costly than traditional solutions. Engineered for SaaS delivery, ServiceWatch encourages IT organizations to shift from monitoring data center silos (servers, networks, storage, applications) to managing end-user business services (CRM, billing, tax payments, fund transfers, etc.). Believing that effective IT 'Starts with the Map,' ServiceWatch's unique technology automatically creates and maintains a run-time map of business services including underlying physical, virtual, network, and storage infrastructures.

Focused on business impact and realizing that IT should monitor only what matters, ServiceWatch's run-time service map enriches event management and monitored information by presentation in the context of the business service, resulting in improved IT change control, rapid problem isolation, and meaningful service health monitoring. While no CMDB is required, ServiceWatch service maps can be imported into BMC Software, CA Technologies, HP, IBM and other ServiceNow applications, making existing CMDBs 'service-aware' with run-time accuracy.

Headquartered in New York and Tel Aviv, ServiceWatch has an installed base of global enterprises, Fortune 10,000 companies, and government/education customers in Europe and North America.