



# ServiceWatch

## User Guide

**Version 3.6**

**September 2014**

© 2014 ServiceNow, Inc.

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, or otherwise, without the prior written permission of ServiceNow, Inc.

No warranty of accuracy is given concerning the content of this publication. To the extent permitted by law, no liability (including liability by reason of negligence) will be accepted by ServiceNow, Inc., its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

**ServiceWatch** is a trademark of ServiceNow, Inc.

Windows is a trademark of Microsoft Corporation.

Other product and company names in this publication may be trademarks of their respective owners.

ServiceNow, Inc. reserves the right to change this publication without notice.

## 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 .....	9
Chapter 1: Getting Started .....	16
Introduction to ServiceWatch .....	16
Advantages of ServiceWatch .....	16
On-Premise ServiceWatch Architecture .....	17
Main Components.....	17
Component interaction during Discovery.....	18
Advantages of Multiple Collectors.....	18
Where to Go From Here .....	19
Chapter 2: Installing ServiceWatch.....	21
Installation Prerequisites .....	21
Ensure All Hardware & Software Requirements Are Satisfied .....	21
Plan Your Collector Configuration.....	21
Create Your Own ServiceWatch Database (if needed) .....	22
On Premise Installation Procedure .....	22
Installing ServiceWatch on Windows.....	22
Installing ServiceWatch on Linux .....	27
Adding HTTPS Support .....	29
Chapter 3: ServiceWatch as a Service .....	30
Main Components.....	30
Architecture of ServiceWatch as a Service .....	30
Collector Requirements .....	30
Registration.....	31
Collector Configuration .....	38
Security Assertion Markup Language .....	38
Chapter 4: Starting & Using ServiceWatch .....	39
Starting ServiceWatch.....	39
Starting and Stopping ServiceWatch Services .....	39
Integration with 3 <sup>rd</sup> party tools.....	40
Screens.....	41
Menu Bar.....	41
Severity Color Coding.....	41
Screen Panels & Panes .....	41
Dashboards .....	42
Dashboard View Toggle Buttons.....	42
Group vs. Business Service Toggle Buttons .....	42

## Table of Contents

Severity Slide.....	42
Business Services .....	42
Dashboard Events .....	43
Dashboard KPIs .....	44
Infrastructure / User Perspective toggle button.....	44
Save and Load Dashboard buttons .....	44
Tile Format Dashboard.....	46
Bubble Format Dashboard .....	47
List Format Dashboard.....	48
Menu Bar Buttons.....	49
Reports window .....	49
Events window.....	50
Dependencies.....	54
Host View .....	62
System Health .....	63
Server Status panel .....	63
Collectors panel .....	64
3 <sup>rd</sup> Party Connectors panel.....	65
Monitoring panel .....	66
Network Discovery panel.....	69
Service Discovery panel .....	71
Chapter 5: Settings .....	73
Settings Menu .....	73
Parameter Types .....	74
Knowledge Base settings .....	74
CI Types, Patterns & Monitors Definitions.....	74
Entry Point Types .....	83
Event Sources/Rules.....	85
Group & Business Service Monitors.....	86
Import / Export .....	89
General settings .....	93
Global Parameters .....	93
License Information .....	105
User Management settings.....	106
Roles.....	106
Users .....	109
System settings .....	111
Alerts .....	111

## Table of Contents

Collectors .....	114
Credentials .....	116
Infrastructure Monitoring.....	121
Monitoring Connectors.....	122
Network Discovery.....	127
System Health .....	128
Virtualization Connectors .....	128
Chapter 6: Configuring Business Services .....	130
Concepts .....	130
Entry Points Pane of the Definitions Panel .....	131
Topology Map .....	131
Business Groups.....	132
Creating and Configuring a New Business Service.....	132
Creating a New Business Service .....	132
Defining Entry Points .....	133
Performing Manual Operations .....	136
Adjusting the Business Service Topology.....	137
Defining Object Impacts on the Business Service .....	140
Creating Technical Business Services.....	149
Root Cause Analysis .....	155
Business Service, Object or Connection Properties .....	156
Viewing the Impact Tree of a Business Service.....	158
Working with Existing Business Services & Groups .....	159
Editing a Business Service .....	160
Topology Map .....	160
Adjusting the Topology Map.....	161
Exporting a Topology Map .....	162
Chapter 7: Configuring Events .....	164
Displaying Events .....	164
Event Processing Flow.....	164
Information Transfer of EMS Events to ServiceWatch .....	165
ServiceWatch Predefined Event Fields .....	165
Integrating ServiceWatch with Your EMS .....	167
Defining the Event Command Line .....	170
Mapping EMS Fields to ServiceWatch Fields .....	170
Extracting and Binding Event Information.....	173
Concepts.....	173
Define the Binding Rule for an Event.....	174

## Table of Contents

Displaying the details of an event in the Unbound Events Table .....	180
Chapter 8: Monitoring Business Services .....	181
Concepts .....	181
Severity Color Coding.....	181
Event Priority.....	182
Viewing All Business Service Statuses at a Glance.....	182
Tile Dashboard .....	183
Bubble Dashboard.....	183
List Dashboard .....	184
View a Business Service or CI.....	184
Map Panel .....	184
Modifying Monitor Attributes.....	185
Aggregate Monitors .....	187
Synthetic Monitors.....	188
KPIs (Key Performance Indicators).....	194
Settings.....	194
Displaying KPIs .....	195
Infrastructure vs. Business Service Perspective.....	195
Table View vs. Thumbnails View .....	196
KPI Filters.....	196
Sorting the KPI columns .....	198
Displaying KPI detail in the Upper Panel.....	199
Chapter 9: Viewing Business Service History .....	201
Concepts .....	201
Viewing a Business Service's History .....	201
Displaying and Comparing Topology Changes and Details .....	203
Chapter 10: Monitoring Networks .....	206
Concepts .....	206
Defining ServiceWatch Network Parameters .....	206
Displaying Network Path Details.....	207
Viewing Properties of a Connection .....	207
Checking the Health of a Network Path.....	210
Chapter 11: Storage Paths.....	212
Defining Storage Path Parameters.....	213
Displaying Storage Path Details .....	214
Chapter 12: Reports .....	217
Report Types .....	217
Reports window .....	217
Sample Reports .....	220

## Table of Contents

Excel Reports Generator .....	223
Download the Reports Generator.....	223
File Extensions for Report Templates and Reports.....	224
Configure Excel Security.....	224
Configure the WMI collector to execute Excel-reports .....	229
Using the Excel SQL Query Reports Generator .....	230
Manual Query tab .....	237
Chapter 13: Troubleshooting.....	238
Windows Management Instrumentation (WMI) .....	238
0x800706BA – RPC Server Unavailable.....	238
0x80070005 – E_ACCESS_DENIED .....	238
ServiceWatch failed to run one or more specific commands.....	239
Verify DCOM Rights.....	240
Verify Security Policy.....	240
Appendix A: Discovery Workflows .....	242
Initial Discovery.....	242
Rediscovery .....	243
Appendix B: Schemas for Tables & Views.....	244
Appendix C: Glossary .....	251
Health Insurance Portability and Accountability Act .....	254
See also Hitachi Storage systems.....	254
Health Level 7.....	254
Appendix D: Adding HTTPS Support.....	265
Configuration Steps.....	265
Copy neebula.jks to the Custom Directory .....	265
Create a key with Java Keytool or import a key into KeyStore .....	265
Generating Keys and Certificates with OpenSSL.....	265
Create a CSR and send it to the Certification Authority .....	266
Loading Certificates with Java Keytool .....	266
Appendix E: ServiceNow CMDB Integration .....	268
Introduction .....	268
Architecture & Functional Overview .....	269
ServiceWatch in on-premise mode.....	271
Installation .....	271
On-Premise Configuration .....	271
ServiceWatch as a Service (SWaaS) .....	273
Installation .....	273
SWaaS Configuration .....	274
Tailoring the Integration .....	275

## Table of Contents

Deleting/Changing/Adding ServiceWatch CIs & Relationships in ServiceNow.....	275
Mapping ServiceWatch-Discovered CIs to ServiceNow CIs .....	276
Mapping a ServiceWatch-Discovered WebSphere to ServiceNow.....	277
Sample XML for CI-to-CI mapping.....	279
Mapping ServiceWatch Relationships.....	280
Viewing ServiceWatch-Discovered Service Models in ServiceNow .....	281
Determining the Relationship Type Key.....	282
Conclusion.....	282
About ServiceWatch: “It all Starts with the Map” .....	282
Supplement A: List of Supported CI Types.....	283
Supplement B: Default Installation mapping.xml file .....	284

# List of Figures and Tables

---

## List of Figures

Figure 1: ServiceWatch Architecture – On-Premise Installation .....	17
Figure 2: Installation Wizard: Welcome & Choose Commands .....	22
Figure 3: Installation Wizard: Choose Install Location & Collector to Server Connection Settings.....	23
Figure 4: Installation Wizard: Database Installation Settings & Installing .....	24
Figure 5: Installation Wizard: Failed to enable .net 3.5.1 & Failed to install PostgreSQL database....	24
Figure 6: Installation Wizard: Finish screen .....	24
Figure 7: Installation Wizard: Installation Aborted screen .....	25
Figure 8: ServiceWatch as a Service Architecture – Server & Database in the Cloud .....	30
Figure 9: ServiceWatch-as-a-Service Registration & Login webpage .....	32
Figure 10: ServiceWatch-as-a-Service Registration & Login webpage .....	33
Figure 11: ServiceWatch Collector Wizard welcome screen .....	34
Figure 12: ServiceWatch Collector Wizard Choose Components screen .....	35
Figure 13: ServiceWatch Collector Wizard Choose Install Location screen.....	35
Figure 14: ServiceWatch Collector Wizard Proxy settings screen .....	36
Figure 15: Add Security token screen .....	37
Figure 16: Installed Collectors Table .....	38
Figure 17: Integration with 3 <sup>rd</sup> party HP uCMDB .....	40
Figure 18: ServiceWatch Menu Bar .....	41
Figure 19: Factory Default Dashboard .....	42
Figure 20: Events panel of the Dashboard.....	43
Figure 21: KPI panel of the Dashboard .....	44
Figure 22: KPIs in the List Format Dashboard .....	44
Figure 23: Saving a Dashboard format.....	45
Figure 24: Load Saved State dialog box .....	45
Figure 25: Save State error message.....	45
Figure 26: ServiceWatch Tile format Dashboard .....	46
Figure 27: ServiceWatch Dashboard – Bubble format.....	47
Figure 28: ServiceWatch Dashboard – List format .....	48
Figure 29: ServiceWatch Dashboard – List format in Standalone mode .....	49
Figure 30: ServiceWatch Menu Bar buttons .....	49
Figure 31: Events window .....	50
Figure 32: Typical CI Types .....	51
Figure 33: Event Details window.....	52
Figure 34: Result of a Dependencies Search using a * wildcard .....	54
Figure 35: Dependencies Search with results filtered .....	54
Figure 36: Dependencies Search – Port Topology .....	55
Figure 37: Dependencies window – Application panel.....	56
Figure 38: Dependencies window – Host panel.....	57

## List of Figures and Tables

Figure 39: Dependencies window – Network panel .....	57
Figure 40: Dependencies window – Storage panel.....	58
Figure 41: Define Change panel (create new change radio button selected) .....	59
Figure 42: Define Change panel (add CI to existing change radio button) .....	60
Figure 43: Dependencies window – Scheduled Changes table .....	60
Figure 44: Update Scheduled Change dialog box .....	61
Figure 45: Topology Map with CIs and Hosts displayed .....	62
Figure 46: Topology Map with only Hosts displayed .....	62
Figure 47: System Health screen – Server Status panel .....	63
Figure 48: System Health screen – Collectors panel.....	64
Figure 49: System Health screen – 3 <sup>rd</sup> Party Connectors panel.....	65
Figure 50: 3 <sup>rd</sup> Party Connectors – Discovery Log window.....	65
Figure 51: System Health screen – Monitoring panel.....	66
Figure 52: System Health screen – Monitoring panel filtered by Message ID.....	66
Figure 53: Full Description in a tool tip.....	66
Figure 54: Expanded CI Type nodes .....	67
Figure 55: Monitoring panel Discovery Log .....	68
Figure 56: System Health screen – Network Discovery panel .....	69
Figure 57: System Health screen – Network Discovery panel filtered by Message ID .....	69
Figure 58: Full Description in a tool tip.....	70
Figure 59: Network Discovery Log .....	70
Figure 60: System Health screen – Service Discovery panel.....	71
Figure 61: System Health screen – Service Discovery panel filtered by Message ID.....	71
Figure 62: Full Description in a tool tip .....	72
Figure 63: Business Service Discovery screen – Discovery Log window .....	72
Figure 64: Settings menu .....	73
Figure 65: CI Type, Pattern and Monitor Definitions window .....	75
Figure 66: Workflow of the CI Type and Pattern definition process .....	77
Figure 67: CI Type Definition window.....	78
Figure 68: CI Table Type – Table Attributes windows.....	78
Figure 69: Choose an icon window .....	79
Figure 70: CI Type Definition – Draft CI Type screen .....	79
Figure 71: Add New CI Type window .....	80
Figure 72: Add New Pattern window .....	80
Figure 73: Add New Monitor window.....	81
Figure 74: Quick Monitor window .....	82
Figure 75: Displaying an Entry Point Type .....	83
Figure 76: Entry Point Type Definition screen .....	84
Figure 77: Events window with Event Rules by Sources tree .....	85
Figure 78: Event Source Definition screen.....	85
Figure 79: Group & Business Service Monitors window.....	86
Figure 80: Business Service Monitor Definition window .....	88

## List of Figures and Tables

Figure 81: Import / Export Knowledge Base window .....	89
Figure 82: Export All Download Link message box .....	89
Figure 83: CI Types Export Download Link message box .....	90
Figure 84: Open, Save, Save as dialog box .....	90
Figure 85: Zip files available for import .....	91
Figure 86: Global Parameters window (with all nodes expanded and sorted) .....	94
Figure 87: Roles window .....	102
Figure 88: Edit Role dialog box.....	103
Figure 89: Edit Role dialog box – Active Directory Users panel.....	103
Figure 90: Role window after adding the DBA role .....	104
Figure 91: License Information table .....	105
Figure 92: License Information bar graph.....	105
Figure 93: Roles windows with tool tips .....	106
Figure 94: Add Role window with Permissions panel.....	107
Figure 95: Add Role window with Responsibilities panel .....	108
Figure 96: Add Role window with Host Permissions panel .....	108
Figure 97: Users window.....	109
Figure 98: Add User dialog box .....	109
Figure 99: Alerts window .....	111
Figure 100: Alert Definition dialog boxes (3 types) .....	112
Figure 101: Collectors window with Add Collector dialog box .....	114
Figure 102: Edit Collector dialog box .....	115
Figure 103: Credentials window .....	116
Figure 104: Credentials Add / Edit scope dialog box .....	117
Figure 105: Add / Edit credentials dialog boxes .....	118
Figure 106: Add / Edit scope dialog box after adding one scope .....	119
Figure 107: Credentials window after adding a Credential .....	120
Figure 108: Monitoring screen with Monitor Scope & Monitor Details dialog boxes.....	121
Figure 109: Monitoring Connectors window with an Add New 3rd Party Connector dialog box .....	122
Figure 110: Add New 3rd Party Monitoring Connector dialog boxes – multiple types.....	123
Figure 111: Network Discovery window .....	127
Figure 112: Virtualization Connectors window with Add New 3rd Party Connector dialog box.....	128
Figure 113: Add New 3rd Party Virtualization Connector dialog boxes – 4 types .....	129
Figure 114: New Business Service option in pop-up menus.....	133
Figure 115: What would you like to do today? Pop-up menu.....	133
Figure 116: Definition panel and Entry Points pane of the Business Service wizard.....	133
Figure 117: Definition panel of the Business Service wizard .....	134
Figure 118: Business Service wizard Entry points pane with URL field.....	134
Figure 119: Entry points pane with Host, DB instance name & Port fields .....	134
Figure 120: Business Service wizard More details fields .....	135
Figure 121: Business Service Topology panel .....	135
Figure 122: Business Service Definition panel in Edit mode.....	136

## List of Figures and Tables

Figure 123: Topology Map with Discovery Messages.....	138
Figure 124: Default impact template for an object with no parent .....	143
Figure 125: Default impact template for an object with one parent .....	143
Figure 126: Default impact template for an object with more than one parent .....	144
Figure 127: Default impact template for an object with 2 parents.....	144
Figure 128: Host impact template .....	144
Figure 129: Hypervisor impact template .....	145
Figure 130: Network impact template.....	145
Figure 131: Storage device impact template .....	145
Figure 132: Business Service Impact Tree of a 2-parent object.....	146
Figure 133: Per Parent Impact Tree for the same 2-parent object.....	146
Figure 134: Cluster impact – Number of Members template.....	147
Figure 135: Cluster impact – Percentage of Members template.....	147
Figure 136: Defining Cluster Impact on its Target (Business service or <name of parent>) .....	148
Figure 137: New Technical Business Service option in pop-up menus.....	149
Figure 138: Technical Business Service – Definition panel with Technical Query Rules pane.....	149
Figure 139: Related groups field in Definition panel .....	150
Figure 140: Technical Business Service priority drop-down list .....	150
Figure 141: Technical Business Service – Technical Query Rules .....	151
Figure 142: Technical Query Rules drop-down lists.....	151
Figure 143: Technical Business Service – More details fields .....	152
Figure 144: Technical Business Service Results .....	152
Figure 145: Technical Business Service – Results panel table display .....	153
Figure 146: Technical Business Service – Element Properties .....	153
Figure 147: Topology Map and Impact Tree when <i>not</i> in Root Cause mode .....	155
Figure 148: Topology Map and Impact Tree in Root Cause mode .....	155
Figure 149: Business Service Properties panel .....	156
Figure 150: Element Properties panel .....	156
Figure 151: Technical Business Service – Technical Query Rules .....	157
Figure 152: Technical Business Service – Ports table.....	157
Figure 153: Connection Properties panel .....	157
Figure 154: Impact Tree panel of a topology Map in View mode .....	158
Figure 155: Right-Click Menus for Groups and for Active and Pending Business Services.....	159
Figure 156: Topology Map panel in Edit mode .....	160
Figure 157: Map manipulation icons in View mode .....	161
Figure 158: Map manipulation icons in Edit mode .....	161
Figure 159: Event Processing Flow.....	164
Figure 160: Empty Events window.....	167
Figure 161: Unbound Events Table in unexpanded recommended Pattern mode .....	168
Figure 162: Unbound Events Table in Tabular mode.....	168
Figure 163: Unbound Events Table in expanded Recommended Pattern mode .....	169
Figure 164: Empty Event Source Definition screen.....	171

## List of Figures and Tables

Figure 165: Event Source Definition window with a rule .....	171
Figure 166: Event Field Mapping dialog box.....	172
Figure 167: New Binding Rule Definition screen .....	175
Figure 168: Binding Rule Definition .....	176
Figure 169: Target type/Field drop-down list .....	177
Figure 170: Field value drop-down list.....	177
Figure 171: Saved Rule Events List.....	178
Figure 172: Missing Field(s) confirmation box.....	179
Figure 173: Event Details table .....	180
Figure 174: Tile Dashboard .....	183
Figure 175: Bubble Dashboard.....	183
Figure 176: Bubble tool tip .....	184
Figure 177: Topology Map in View mode .....	184
Figure 178: All Groups & Business Services tree.....	186
Figure 179: Typical Monitor Modification screen.....	186
Figure 180: Check Monitor Results – Events List .....	186
Figure 181: Add New Aggregate Monitor option .....	187
Figure 182: Add a new Aggregate Monitor screen .....	187
Figure 183: Check Monitor Results – Events List .....	188
Figure 184: Add New Synthetic Monitor option .....	188
Figure 185: Add a new Synthetic Monitor screen .....	189
Figure 186: Files extracted from ServiceWatchRecorder.zip.....	190
Figure 187: Synthetic Transaction Recorder wizard's Welcome screen.....	190
Figure 188: Content, Conditions & Parameters of the Synthetic Transaction Recorder wizard .....	191
Figure 189: Total transaction time and Threshold levels in milliseconds.....	192
Figure 190: File extension deletion button.....	192
Figure 191: Search for next-occurrence button.....	192
Figure 192: Select a Collector dialog box.....	192
Figure 193: KPI Monitoring Enabled flag .....	194
Figure 194: Business Service Topology Map in Edit mode .....	194
Figure 195: Edit Monitor Scheduler dialog box .....	195
Figure 196: Displaying KPI thumbnails of the first 4 of 19 monitors .....	195
Figure 197: Table View for KPI charts .....	196
Figure 198: KPI filters .....	196
Figure 199: KPI Name filter .....	197
Figure 200: KPI Severity filter.....	197
Figure 201: KPI Entity Name filter.....	197
Figure 202: KPI display after dragging 4 CPU Utilization Monitors into the topology Map area .....	199
Figure 203: Comparing the KPI graphs of 3 CPU monitors .....	199
Figure 204: History panel for the previous week.....	201
Figure 205: History pane with timelines for related business services .....	204
Figure 206: History Compare on <business service name> pane (top only, topology <i>not</i> shown) ....	204

## List of Figures and Tables

Figure 207: Network Path panel .....	207
Figure 208: General Properties of an object in the Network Path .....	208
Figure 209: Ports screen – Properties table pop-up .....	208
Figure 210: Connection Properties – Network Path .....	209
Figure 211: Business Service Properties in Network Path panel .....	209
Figure 212: Network Status in the Impact Tree.....	210
Figure 213: Storage Path panel in View mode.....	212
Figure 214: Business Service topology with a Storage Array (NetApp FAS270) .....	214
Figure 215: Show storage path option in Connection right-click pop-up menu.....	214
Figure 216: Path selection box.....	214
Figure 217: Storage Path panel.....	215
Figure 218: Storage device data displayed in right pane .....	215
Figure 219: Reports window .....	218
Figure 220: Checkboxes for Business Services and Change types .....	219
Figure 221: Schedule report days-of-the-week settings.....	219
Figure 222: Schedule report day-of-the-month settings .....	219
Figure 223: Saved Reports tool tip.....	220
Figure 224: Number of opened events report.....	220
Figure 225: SLA Compliance Report.....	221
Figure 226: Business service status report .....	221
Figure 227: Topology change report.....	222
Figure 228: Business Service Status Distribution report.....	222
Figure 229: Four Excel Reports Generator files extracted from the zip file .....	223
Figure 230: Extraction path for the ServiceWatch Query Builder .....	224
Figure 231: Excel Options screen – Customize Ribbon option .....	226
Figure 232: Macro Security option of the Developer panel .....	226
Figure 233: Trust Center dialog box .....	227
Figure 234: Trusted Locations option of the Trust Center screen .....	229
Figure 235: Trusted Locations Path list.....	229
Figure 236: WMI Collector in the Windows Services screen .....	230
Figure 237: Properties window – General panel and Log On panel .....	230
Figure 238: Graphic SQL Query Builder tab of the Reports Generator Excel application .....	231
Figure 239: Creating links (joins) between database tables & displaying Link Properties .....	232
Figure 240: Expression column in the Main panel of the graphic Query Builder .....	232
Figure 241: Sample query built graphically.....	234
Figure 242: Report Name table in the Data tab.....	235
Figure 243: Select file to upload by <IP address> window .....	235
Figure 244: Verification that an uploaded Report is one of the listed Report Types .....	236
Figure 245: ServiceWatch Credentials dialog box.....	237
Figure 246: WMI Ctrl > WMI Ctrl Prop. > Security for root > Adv. Security...> Permission Entry....	239
Figure 247: Local Security Policy > Component Serv. > Computer Prop. > Launch & Activation....	240
Figure 248: Local Security Policy > Debug programs Properties .....	241

## List of Figures and Tables

Figure 249: Graphic illustration of how the integration works .....	270
Figure 250: Contents of the Neebula > ServiceWatch > server > cmdb > sn folder .....	271
Figure 251: Business Service right-click pop-up menu .....	272
Figure 252: List of extracted files .....	273
Figure 253: Table of CI Attributes in the CI Type Definition screen.....	277
Figure 254: Map options dialog box for E-banking View .....	281
Figure 255: E-banking Business Service as displayed in ServiceNow.....	281
Figure 256: ServiceNow Key extraction .....	282

## List of Tables

Table 1: Alphabetical list of Event Detail Keys.....	53
Table 2: Alphabetical list of Entity Types .....	75
Table 3: Right-click menu options.....	76
Table 4: Global Parameters.....	96
Table 5: Topology Map Adjustment Options for Objects .....	139
Table 6: Topology Map Adjustment Options on Connection Lines .....	140
Table 7: Group/Business Service Manipulation .....	159
Table 8: Topology Map manipulation actions.....	161
Table 9: Predefined Event Fields.....	166
Table 10: Business Service History actions .....	203
Table 11: Built-in Schemas for ServiceWatch Reports.....	244
Table 12: Glossary .....	251

# Chapter 1: Getting Started

---

This chapter contains the following topics:

- [INTRODUCTION TO SERVICEWATCH](#)
- [ADVANTAGES OF SERVICEWATCH](#)
- [ON-PREMISE SERVICEWATCH ARCHITECTURE](#)
- [WHERE TO GO FROM HERE](#)

## 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.

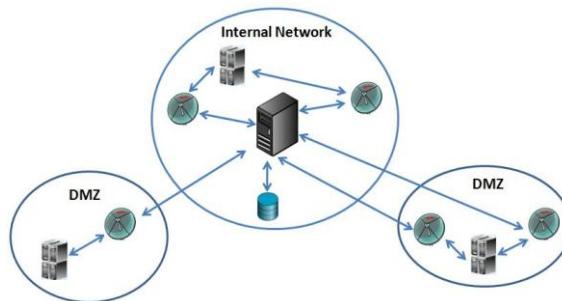
ServiceWatch does not replace the event management and monitoring tools currently installed in your IT environment. Instead, ServiceWatch integrates with them to provide a dynamic Business Service Management picture of events. In addition to providing top-down discovery and a real-time updated topology 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.
- Windows machines and Linux/Unix machines need separate collectors.

# 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](#).

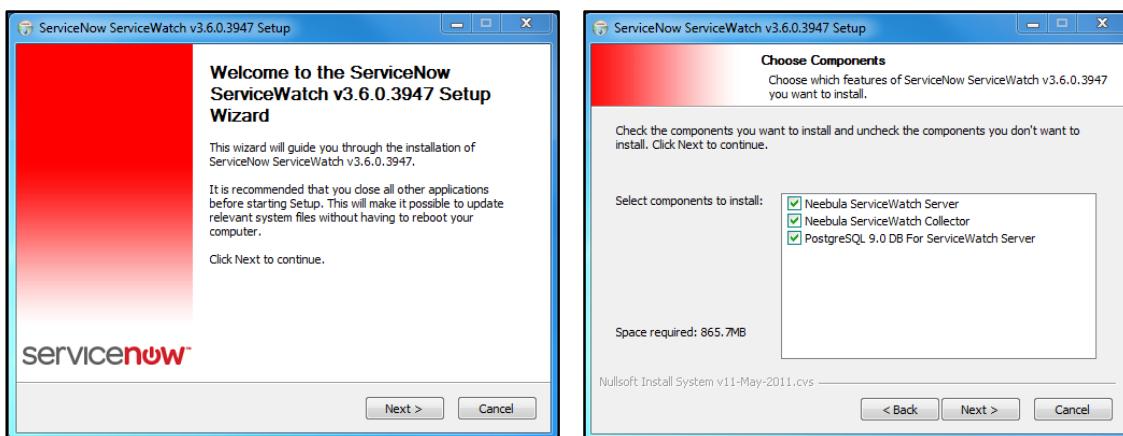
This section contains the following procedures:

- [Installing ServiceWatch on Windows](#)
- [Installing ServiceWatch on Linux](#)

### 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**

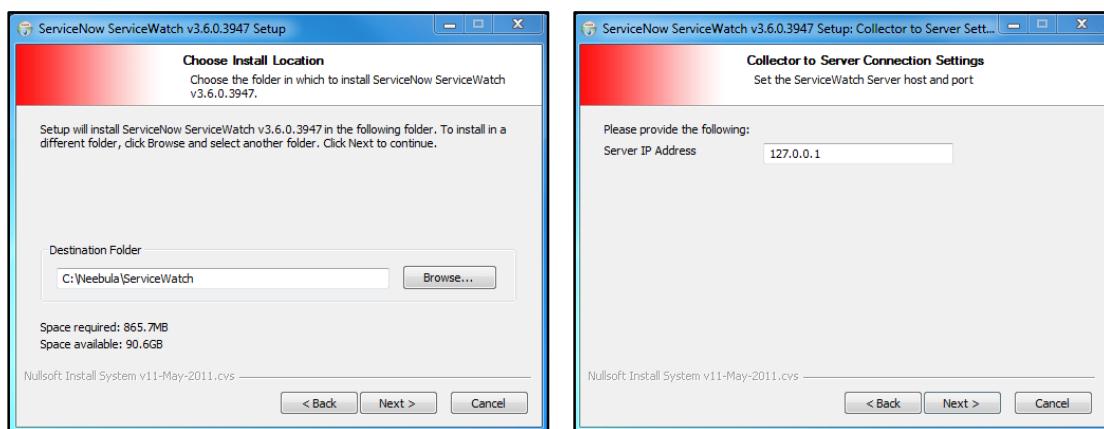


3. The **Choose Components** screen of the wizard is displayed for a new installation but not displayed for an upgrade.
- The ServiceWatch Collector checkbox is checked. If your configuration does not include a collector on this Server machine, uncheck this box.
  - ✓ For every other Windows machine 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.

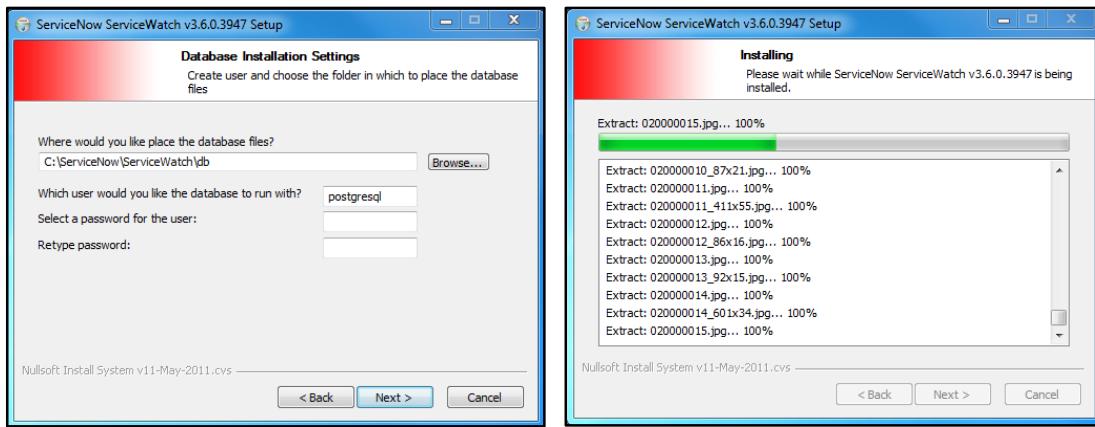
**Figure 3: Installation Wizard: Choose Install Location & Collector to Server Connection Settings**



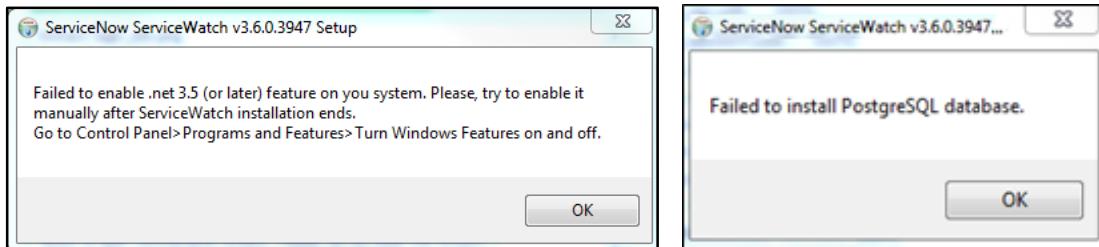
4. The **Choose Install Location** screen is displayed for a new installation but not displayed for an upgrade. If displayed, browse for the desired **Destination Folder** location and click **Next**.
5. The **Collector to Server Connection Settings** screen is displayed for a new installation but not 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.

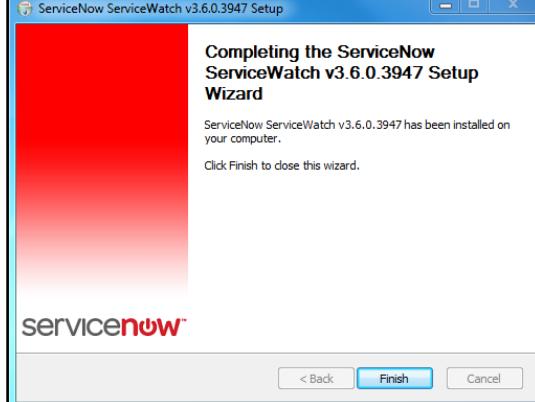
When you click **Next**, the **Installing** screen is displayed.

**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.

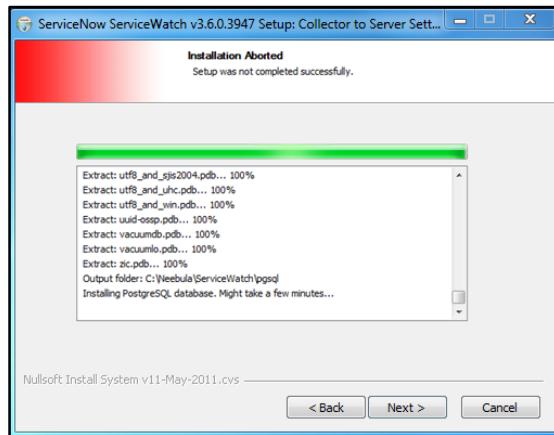
**Figure 5: Installation Wizard: Failed to enable .net 3.5.1 & Failed to install PostgreSQL database**

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:

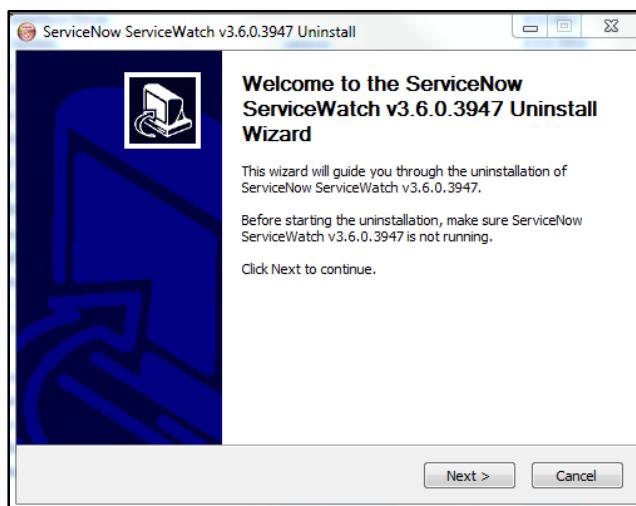
**Figure 6: Installation Wizard: Finish screen**

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

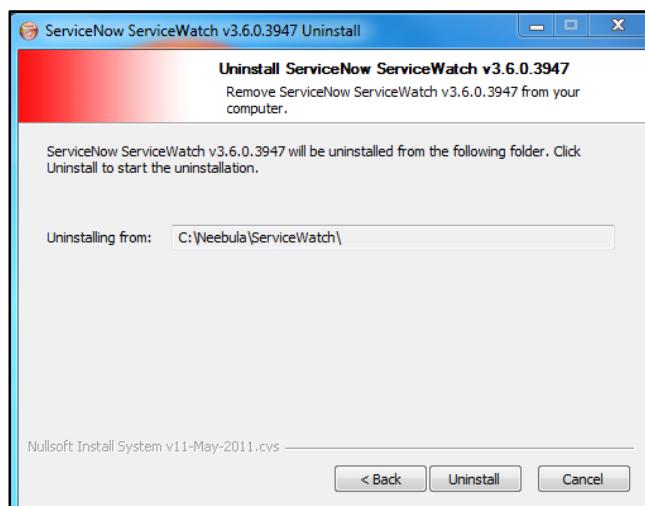
**Figure 7: Installation Wizard: Installation Aborted screen**



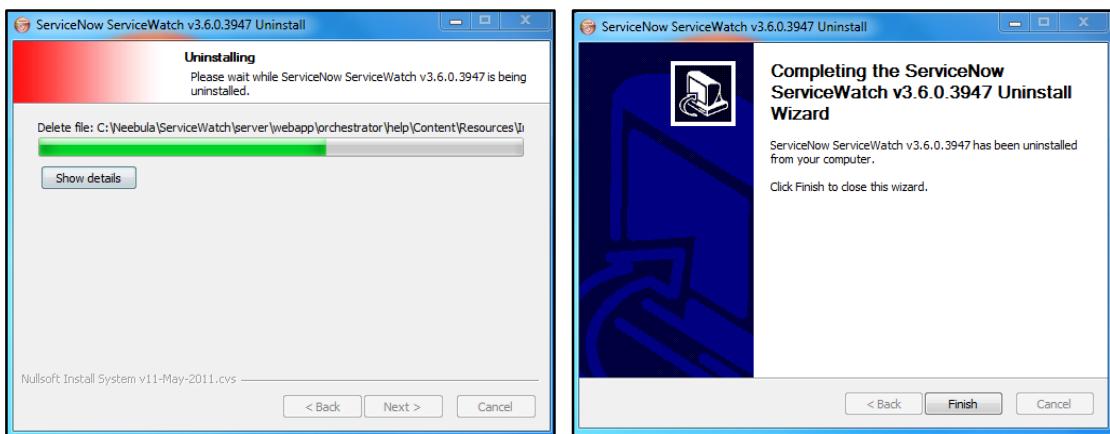
11. To uninstall ServiceWatch, use the Uninstall or change a program utility in the Windows Control Panel. When you click the Uninstall/Change button, the Welcome screen of the ServiceNow ServiceWatch Uninstall Wizard is displayed.



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 neebula
                --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 neebula
                --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](http://wiki.eclipse.org/Jetty/Howto/Configure_SSL)

To enable ServiceWatch to provide HTTPS support and to see instructions for adding a certificate, see [APPENDIX D: ADDING HTTPS SUPPORT](#).

# Chapter 3: ServiceWatch as a Service

This chapter contains the following topics:

- [MAIN COMPONENTS](#)
- [ARCHITECTURE OF SERVICEWATCH AS A SERVICE](#)
- [COLLECTOR REQUIREMENTS](#)
- [REGISTRATION](#)
- [COLLECTOR CONFIGURATION](#)

**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.

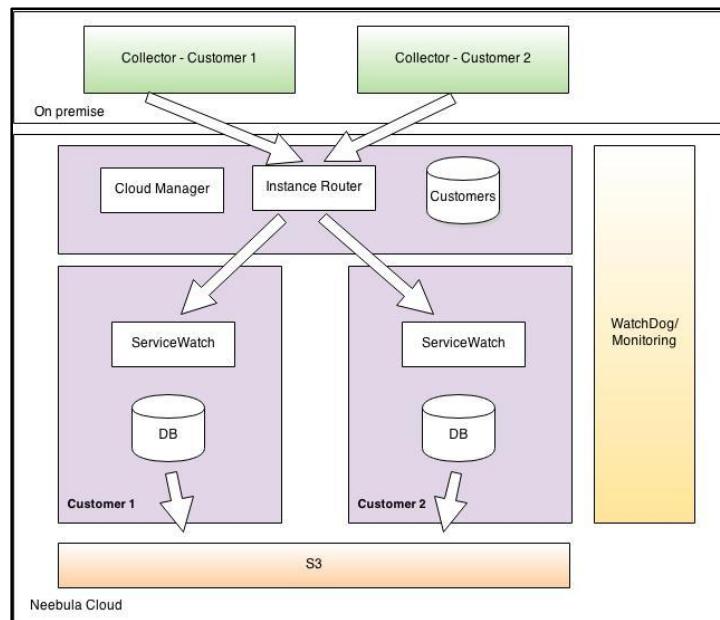
## Main Components

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***

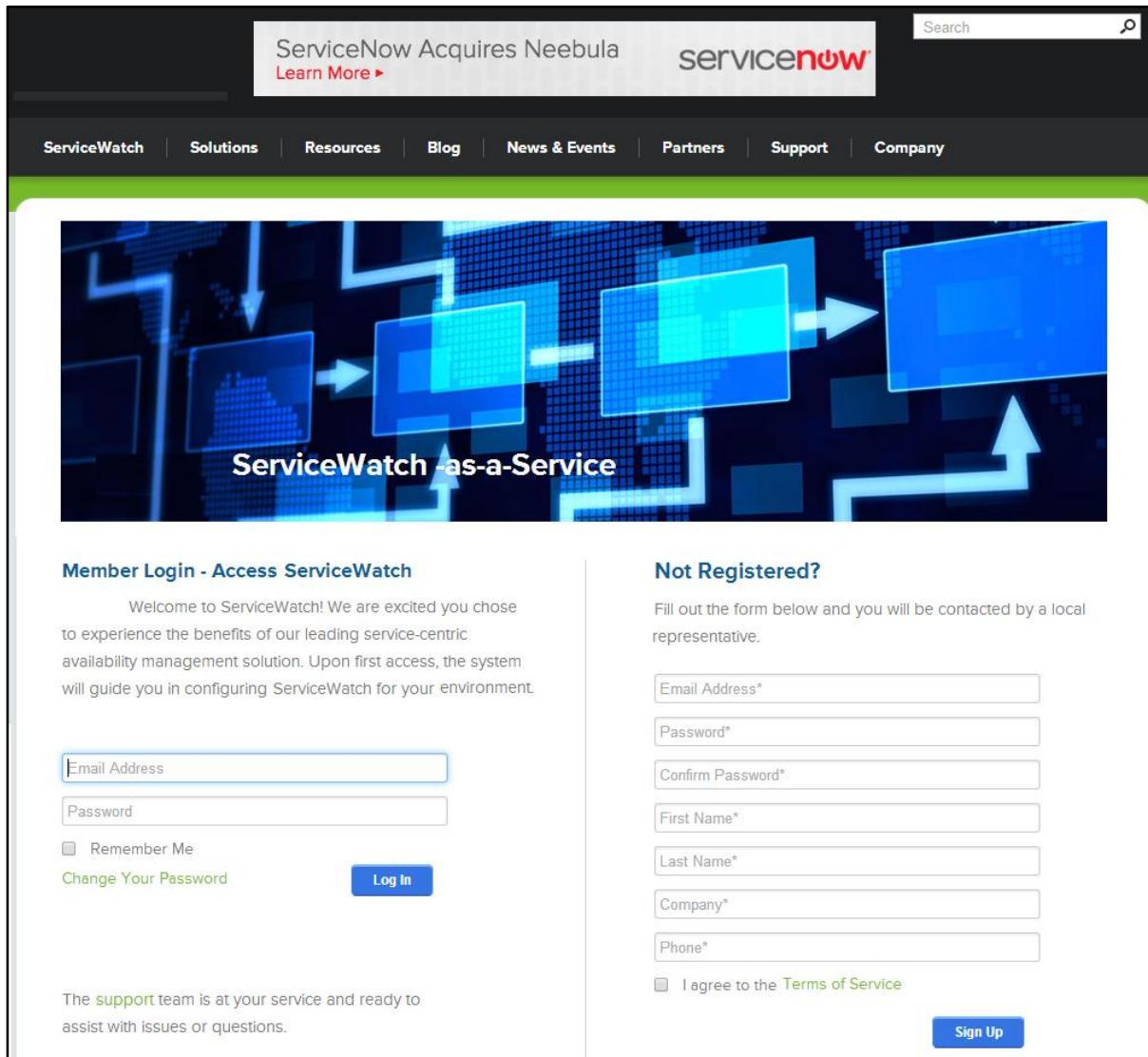
Apply the information presented in [Advantages of Multiple Collectors](#) on page [18](#) to determine:

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

## **Registration**

Enter [servicewatch.servicenow.com](http://servicewatch.servicenow.com) in your browser to access the ServiceWatch-as-a-Service webpage.

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



**Member Login - Access ServiceWatch**

Welcome to ServiceWatch! We are excited you chose to experience the benefits of our leading service-centric availability management solution. Upon first access, the system will guide you in configuring ServiceWatch for your environment.

Email Address

Password

Remember Me

[Change Your Password](#)

**Log In**

The support team is at your service and ready to assist with issues or questions.

**Not Registered?**

Fill out the form below and you will be contacted by a local representative.

Email Address\*

Password\*

Confirm Password\*

First Name\*

Last Name\*

Company\*

Phone\*

I agree to the [Terms of Service](#)

**Sign Up**

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***

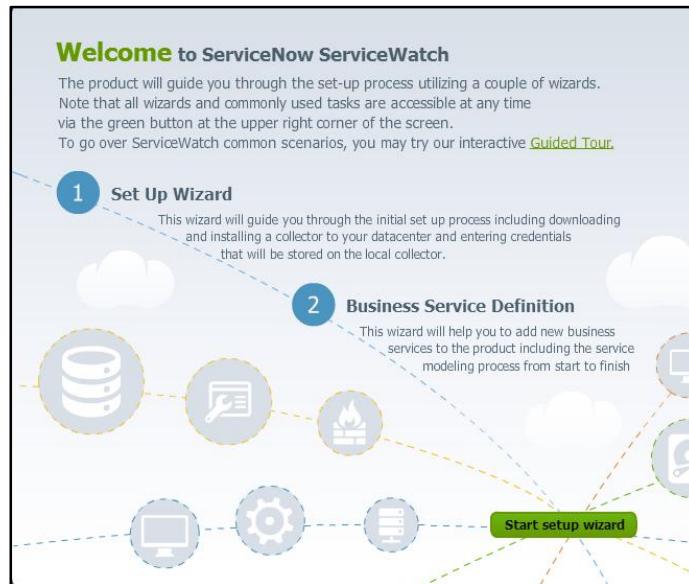
Your 30 day trial is about to begin.

We are now preparing your personalized ServiceWatch environment and you will soon receive an email with instructions on how to access it.

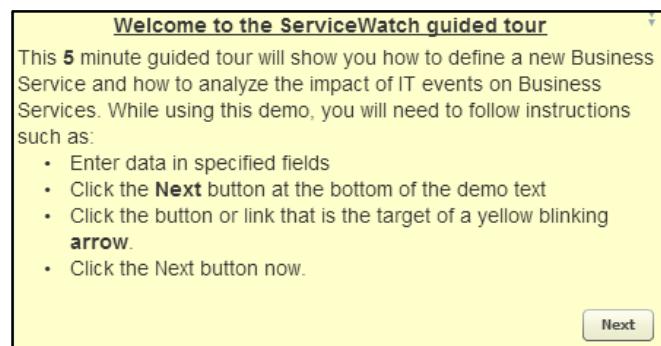
You should receive an email confirmation of your Registration after a few minutes. When you receive the confirmation, fill in your email address and password on the left side of the [servicewatch.servicenow.com](http://servicewatch.servicenow.com) webpage and click the **Log In** button.

The following window will be displayed:

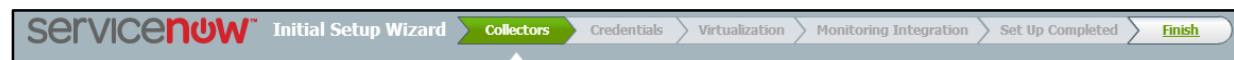
Figure 10: ServiceWatch-as-a-Service Registration &amp; Login webpage



Enjoy the [Guided Tour](#)



and then click the **Start setup wizard** button. The wizard will guide you through the following steps:



Installed collectors:	
Name	Status

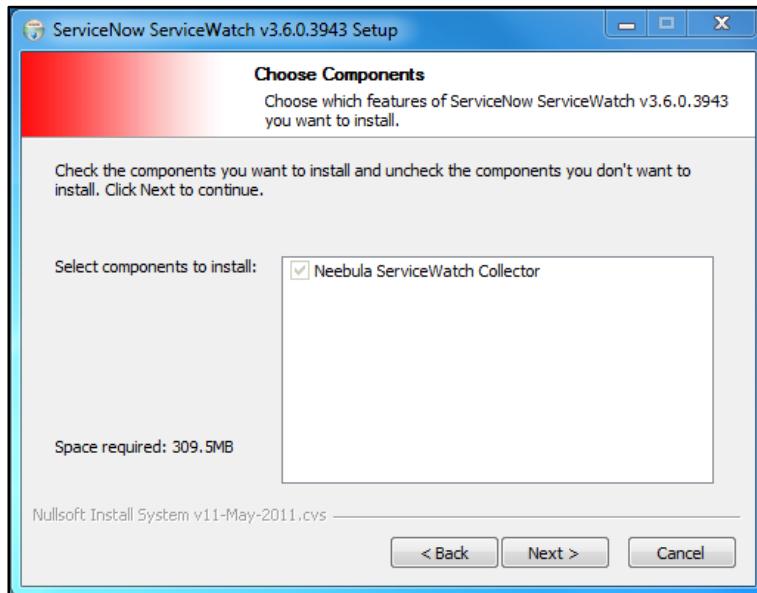
[Next](#)

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**

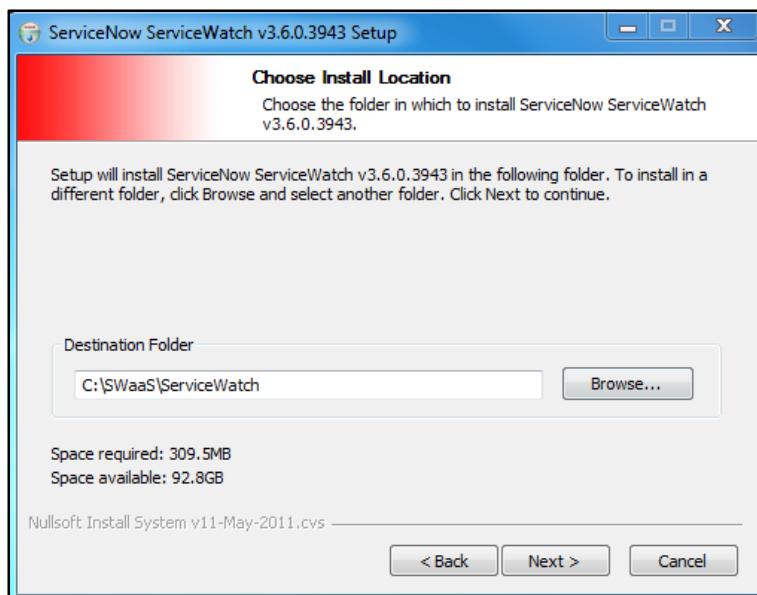


Click **Next** to display the **Choose Components** screen.

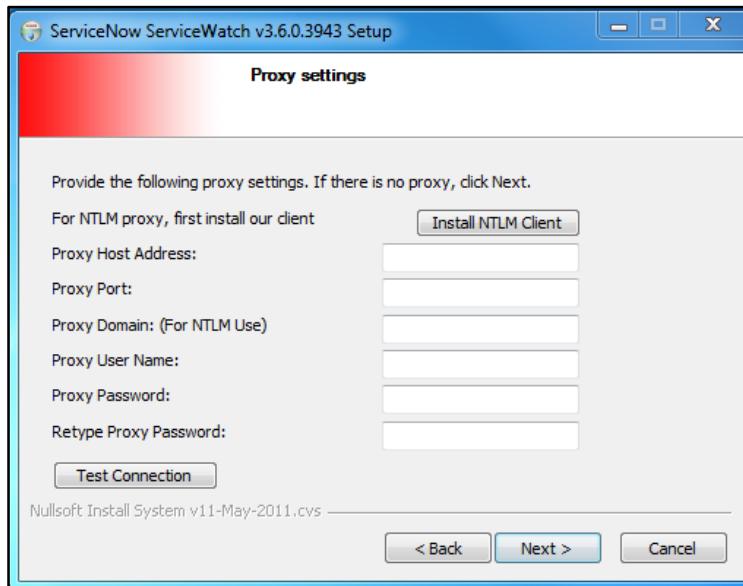
**Figure 12: ServiceWatch Collector Wizard Choose Components screen**

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**

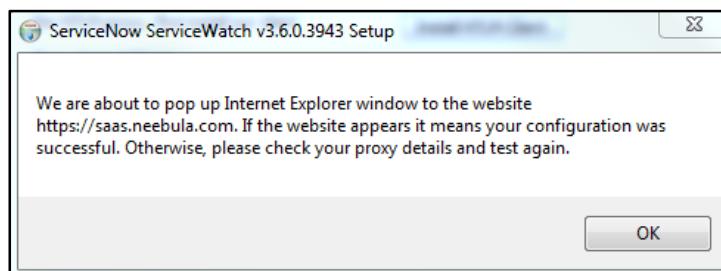
If you are *not* using a proxy, skip this screen by clicking **Next**.

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.

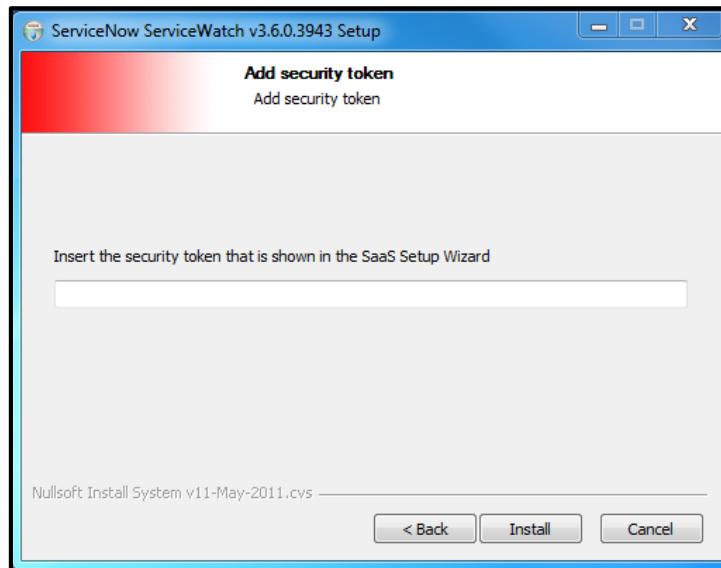
If you *are* using NTLM (NT LAN Manager) authentication, click the **Install NTLM client** button to display an NTLM client installation wizard in a separate window. Follow that wizard's instructions.

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.

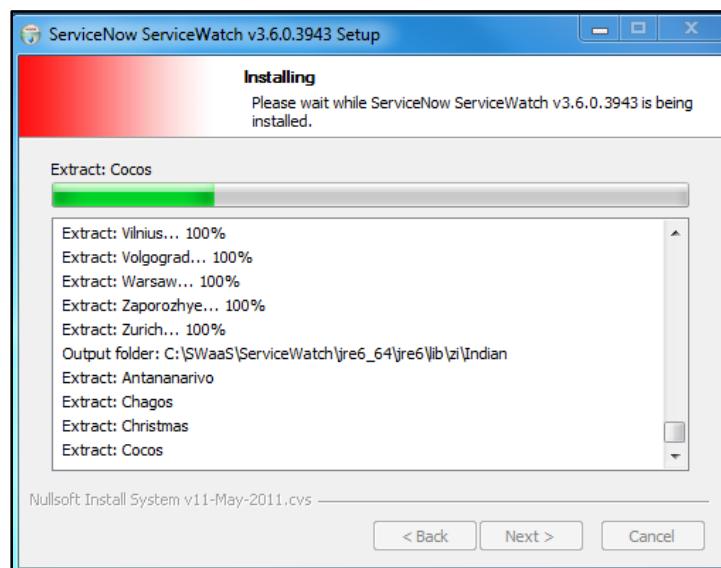
In all 3 cases (no proxy, NTLM proxy, regular proxy) you should click **Test Connection**. An Internet Explorer window pop-up warning is displayed.



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**



The screenshot shows a configuration interface for ServiceNow ServiceWatch. The title is "Collectors". It contains instructions for downloading the collector application and inserting a security token. It also shows a table titled "Installed collectors:" with two entries:

Name	Status
T61-Izzy (172.16.1.105)	Active
T61-Izzy (172.16.1.105)	Inactive

At the bottom right of the table is a "Next" button.

## 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
- Integration with 3rd party tools
- Screens
- Dashboards
- Menu Bar Buttons
- System Health

## 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 3<sup>rd</sup> party tools

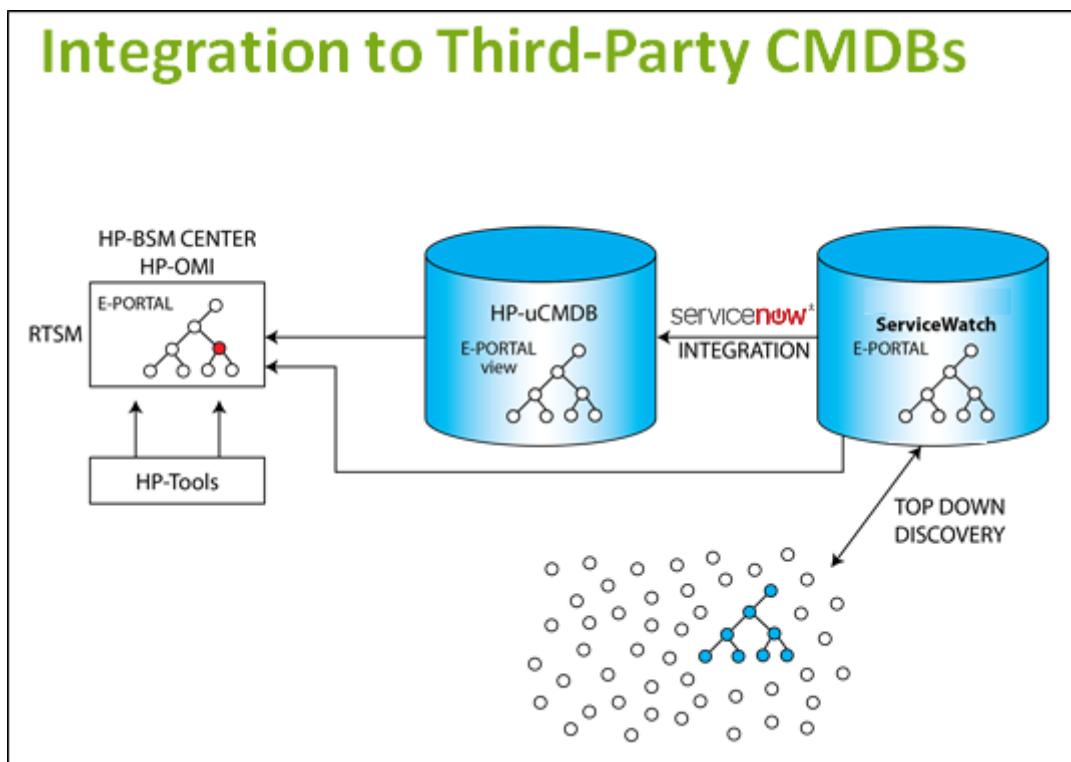
ServiceWatch integrates with other event management and monitoring tools to indicate how events impact business services. **Critical, Major, Minor, Warning or Information** severity is assigned to each event. The list of integrated products includes: GroundWork, HP Operations Manager, Netcool, SCOM, 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 3<sup>rd</sup> 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**

The screenshot shows the ServiceNow dashboard with a 'Bubble' view mode selected. The top navigation bar includes 'Dashboard', 'Reports', 'Events', 'Dependencies', and other icons. On the left, there's a search bar and a sidebar with sections for 'Active' (59) and 'Pending' (46) services. The main area displays a grid of service icons, some labeled with names like 'apache', 'berlin', 'BizTalk', etc., and others with more detailed descriptions like 'TBS: Windows 2008'. Below this grid is a table for 'Events' and 'KPI', showing 38 Critical, 14 Major, 10 Minor, and 0 Warning events, along with a list of recent event logs.

## 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

Date and Time	Severity	Event	Priority	Host
07/29/2014 6:41:22 PM	Critical	CPU usage (100%), is above specified threshold	62	V-RHEL-5-32-WAS01.localhost.localdomain
07/29/2014 6:48:53 PM	Minor	CPU usage (57%), is above specified threshold	2	V-W2K3-SQL-SIIS
07/29/2014 6:46:22 PM	Minor	CPU usage (62%), is above specified threshold	10	localhost.localdomain
07/29/2014 6:46:16 PM	Minor	CPU usage (67%), is above specified threshold	2	V-W2K8-EX2010
07/29/2014 6:48:07 PM	Major	CPU usage (82%), is above specified threshold	17	V-W2K3-32-QA

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  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.

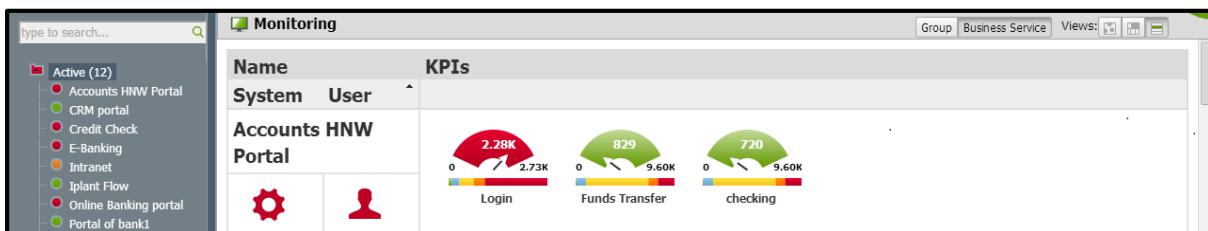
**Figure 21: KPI panel on the Dashboard**



KPI Name	Severity	Entity Name	Value	Monitor Type
(1202748) Free sp...	Critical	V-W2K3-NIGHT	5 [%]	Host
(1056302) Free sp...	Information	V-W2K8-R2-WMI02	71 [%]	Host
(1056304) Free sp...	Minor	V-W2K8-R2-WMI02	47 [%]	Host

KPIs are automatically displayed in the List Format Dashboard.

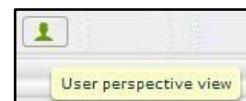
**Figure 22: KPIs in the List Format Dashboard**



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.

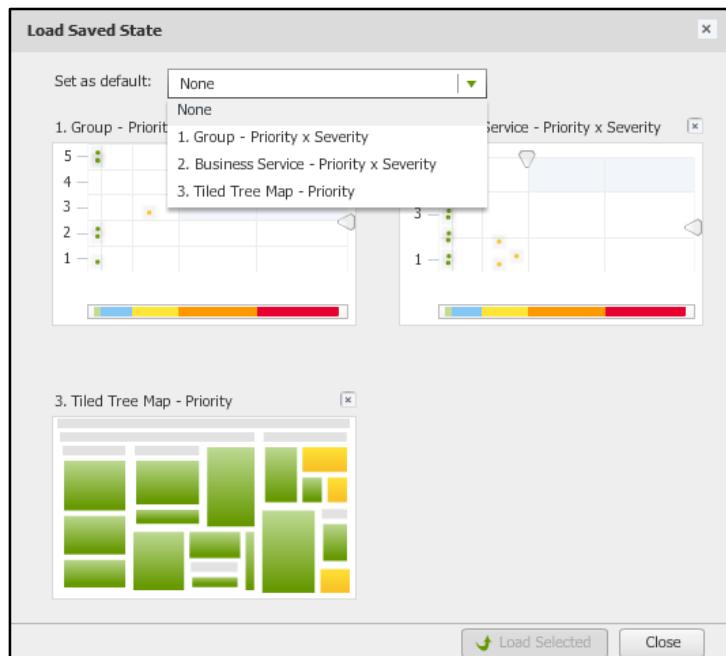


## Save and Load Dashboard buttons

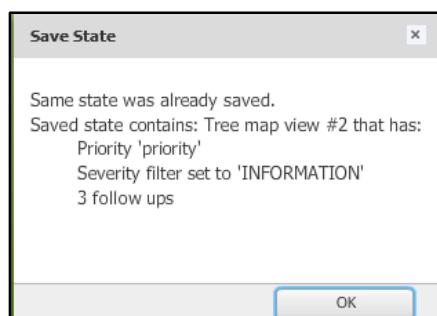
Up to 4 Dashboard formats can be saved. Clicking the  button displays the **Save State** dialog box. You can modify the automatically displayed name in the text box. Clicking the  button in the dialog box will save the format as State 1, 2, 3 or 4 with the specified name.

**Figure 23: Saving a Dashboard format**

Clicking the 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 . Click 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**

The screenshot shows the ServiceWatch interface with the following details:

- Header:** Logged in as admin Log out, Dashboard, Reports, Events, Dependencies, and various navigation icons.
- Left Sidebar:**
  - Looking for ... search bar.
  - Active (59) section with a tree view of business services:
    - apache on solaris zone
    - berlin
    - BizTalk
    - dangling CI test
    - google.com
    - jira/5
    - Performance
    - dans database (29)
    - from shomi or hall (3)
    - ronie testing (13)
    - test (3)
    - testing (7)
    - Yotam simulation (4)
  - Pending (46) section with a tree view of pending items:
    - 148
    - 84
    - Analysis Services
    - ap
    - Biztalk 2009
    - Citrix 5
    - EBS V11
    - EBS V12
- Monitoring Panel:**
  - Severity: Priority (red, orange, yellow, green).
  - Display: 59 of 59 Follow up business services: Specified follow up business services: None.
  - Priority: Group, Business Service, Views: List, Grid, Details, Legend, Load, Save.
  - Active business services are displayed as tiles in a grid:
    - QA Domain Group, QA Applications, Microsoft, IIS, Exchange, SharePoint, EBS, and QA Inventory groups.
    - Production Domain Group, Production, and TBS: Windows 2008, Vmw are Sql, Production ESX, Production Serve, Microsoft Cluster, Hudson, Wi ki, vCenter, TBS-Unix, VMs, sniffer on 124, Java TBS, HA Proxy, Windows Cluster (2), simulation-test, Exchange 2007 CCR, Exchange 2010, and Wi ndow.
    - ronie testing, 10.1.1.12 4 - collector, 10.1.1.12 4 - collector, mssql - TBS, TBS: MS SQL, suse, apache, WAS Trade, Yotam simulation, live demo, yotam -simu, sim2, hop1, google.co m, jira/5, and Performance.
    - from shomi or h, Microsoft Cluster, Composer + TAM, berlin, BizTalk, dangling CI test, apache on solaris zone, and Hudson/2.
- Events and KPI:**
  - Events tab: Date and Time, Severity, Event, Priority, Host. Last event: 07/28/2014 4:38:27 PM, Critical, Used disk space on drive / is 100%, Priority 62, Host V-RHEL-5-32-WAS01.localhost.localdomain.
  - KPI tab: 38 Critical, 14 Major, 10 Minor, 0 Warning, 1 - 5 out of 62 events.

## 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).

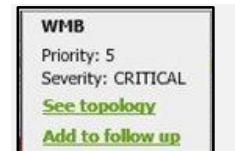


Figure 27: ServiceWatch Dashboard – Bubble format

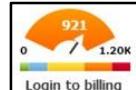
Date and Time	Severity	Event	Priority	Host
07/28/2014 6:28:40 PM	Critical	CPU usage (100%), is a...	67	localhost.localdomain
07/28/2014 6:12:50 PM	Critical	Used disk space on driv...	62	V-RHEL-5-32-WAS01.localdomain
07/28/2014 6:05:40 PM	Critical	kuku	61	rhel-physical.qa.lab.local
07/28/2014 6:23:27 PM	Critical	CPU usage (141%), is ab...	60	V-W2K3-32-ORA101
07/28/2014 6:08:47 PM	Critical	Free disk space percenta...	59	V-W2K3-32-WAS01

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

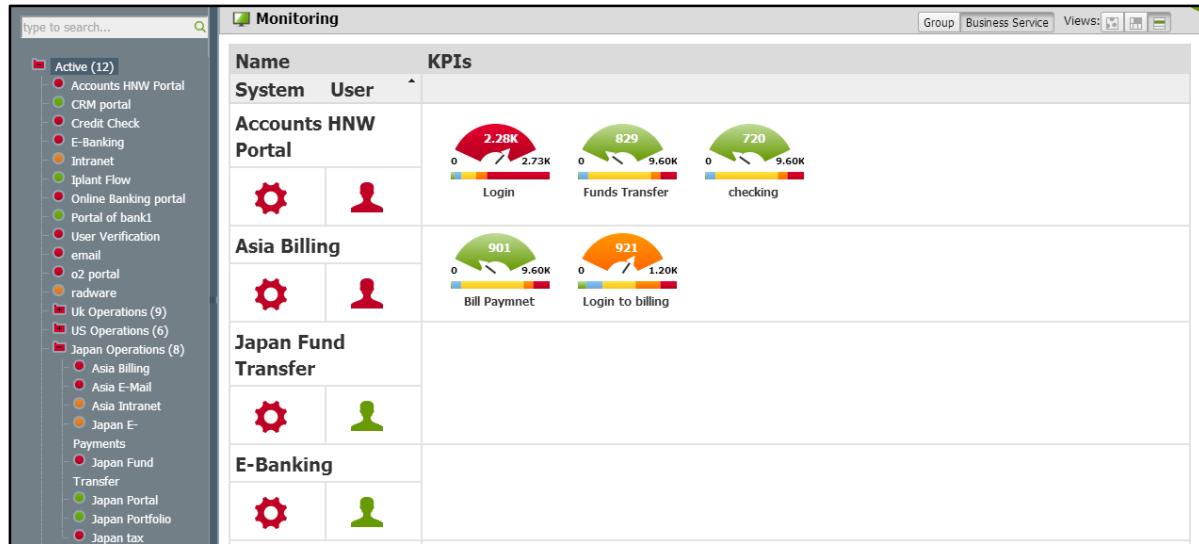
Figure 28 illustrates the desktop/laptop List Format dashboard that displays each active

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.

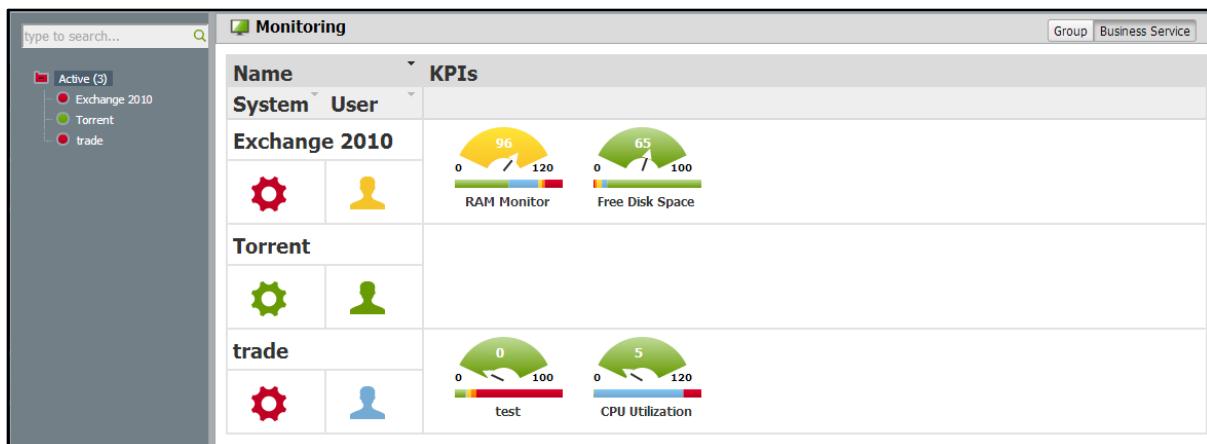
If Critical severities are associated with higher numbers, the red end of the threshold bar is on the right. If Critical severities are associated with lower numbers, the red end is on the left.

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**

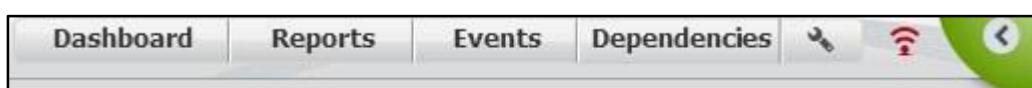


## **Menu Bar Buttons**

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 **Reports** 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 screenshot shows the ServiceNow Events window. At the top, there are navigation links: Dashboard, Reports, Events (which is selected and highlighted in green), Dependencies, and a search icon. Below the header, there are several filter options: View (Showing events from all dates), Events state (All), CI/CI type (All CI Types), and a search field for Filter by event description or host. To the right of these filters is a 'Choose columns' button. The main area is a table with the following columns: Date and Time, Severity, Event, Priority, EMS, Host address, and State. The table lists various events, such as low disk space on drives C and E, and a transaction exchange issue. At the bottom of the table, there is a message: '9 new events are waiting'. Navigation controls include page numbers (1-5), a '200 Pages' link, a 'Rows in Page' dropdown set to 50, and an 'Estimated events count: 10000' link.

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:

This dialog box allows users to specify a date range. It features two radio buttons: one for 'From' (selected) and one for 'Show events from all dates'. The 'From' section includes a calendar icon, a date input field showing '01/01/2014', a time input field showing '00:00:00', and up/down arrows for hours, minutes, and seconds. The 'To' section is similar, showing '15/01/2014' and '23:59:59'.

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](#).

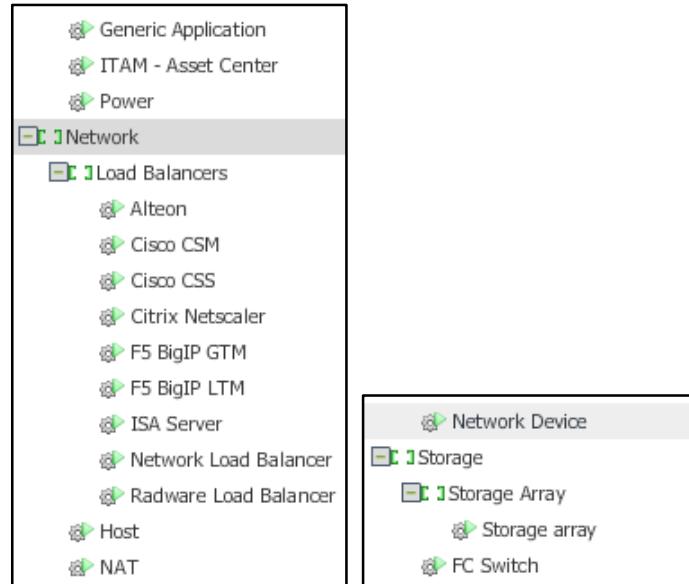
Figure 32: Typical CI Types

All CI Types ▾ Filter by event desc

Filter by:  CI type  CI  
You may use "\*" or "." as wildcards

Search CI type

- All CI Types
  - Applications
    - Application Servers
      - Data Power
      - Data Power Domain
      - HP uCMDB
      - Jboss
      - Jboss module
      - Jrun
      - Jrun WAR Inc
      - Oracle iAS
      - Oracle iAS Web module
      - Tomcat
      - Tomcat WAR
      - Weblogic
      - Weblogic PS
  - Business Integration Software
    - BizTalk
    - BizTalk Orchestration
    - CICS Transaction Gateway
    - HP Quality Center
    - IBM CICS
    - IBM WMB Http Listener
    - IBM WebSphere MQ
    - IBM WebSphere MQ Queue
    - IBM WebSphere Message Broker
  - Database Servers
    - DB2
    - MS SQL database
  - Documentum Brava Job Processor
  - Documentum Brava License Server
  - Documentum Broker
  - Documentum Content Server
  - Fast Index Server
  - HP Operations Manager
  - HP SM Index Server
  - HP SM KnowledgeBase
  - HP Service Manager
  - MS Dynamic CRM Component
  - Peoplesoft Application Server
  - SAPApplicationServer
  - SAPSystem
  - ServiceWatch
  - Tibco Hawk
  - Mail Services
  - Mail Seal
  - Microsoft Exchange
  - Microsoft SharePoint
  - Oracle Database
  - Oracle Forms Engine
  - Oracle Forms UI
  - Oracle Fulfillment Server
  - Oracle HTTP Server
  - Oracle Listener
  - Oracle Metric Client
  - Oracle Metric Server
  - Oracle Notification Server
  - Oracle OACORE Server
  - Oracle OAFM Server
  - Oracle Process Manager
  - Oracle Tnslsnr Engine
  - Oracle Weblogic JMS Queue
  - Tibco ActiveMatrix Business Works
  - Tibco ActiveMatrix Business Works Process
  - Tibco EMS Queue
  - Tibco Enterprise Message Service
  - WMB Flow
  - Weblogic JMS Server
  - AD\_Forest
    - Active Directory Domain Controller
    - CA Policy Server
    - CA Site Minder
    - HA Proxy
    - IIFP
    - LDAP DB
    - Sun Directory Proxy Server
    - Sun LDAP Server
  - Enterprise Applications
    - Citrix Application Icon
    - Citrix Collector
    - Citrix XenAPP or Presentation Server
  - Connect-It Service
  - Control-M
  - Documentum Brava Job Processor
  - Cisco UCS Blade Server
  - Cisco UCS Chassis
  - Cisco UCS Manager
  - Groundwork Monitoring
  - Hitachi Manager
  - Portals
    - SharePoint
    - SharePoint Service
    - Websphere Portal
  - Web Servers
    - Apache Web Server
    - IIS
    - Inetinfo
    - Sun iPlanet Webserver
    - Virtual Directory
    - Generic Application



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.

Port check failed on 10.1.0.148:4321. Connection refused: connect. Host is	52	NEEBULA
Transaction www.neebula.com took 2422.0 msec	0	NEEBULA
Transaction www.neebula.com took 3261.0 msec	<b>Port check failed on 10.1.0.148:4321. Connection refused: connect. Host is reachable by ping</b>	

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

**Figure 33: Event Details window**

Event Details	
Key	Value
Business Service Name	Exchange 2010
Ems System	NEEBULA
Event Creation Time	15/01/2014 9:09:16
Event type	REGULAR
ID	66729301
Message Key	Exchange 2010_76E0B784-D780-462A-9A17-C713EC57DB92_Match
Monitor id	76E0B784-D780-462A-9A17-C713EC57DB92
Monitor name	exchange
Monitor type	SYNTHETIC_MONITOR
Neebula Event Time	15/01/2014 10:49:44
Priority	51
Resolution State	NEW
Severity	CRITICAL
Text	Expected response code for /owa/ev.owa is: 200 but was: 440

OK

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 <b>Event Priority</b> on page <a href="#">43</a> or page <a href="#">182</a>
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

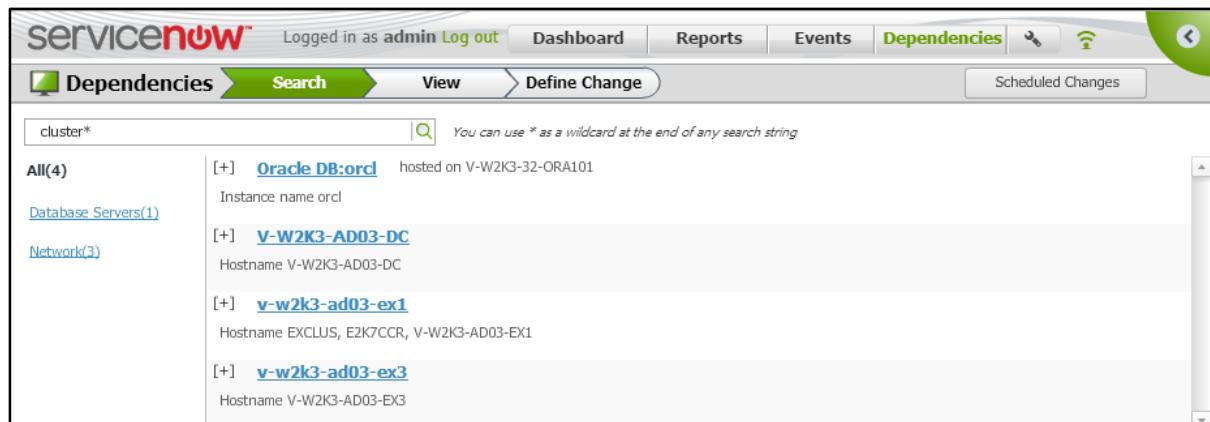
This feature enables you to search for a CI and then view its dependencies map and/or define changes to that CI.

### 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

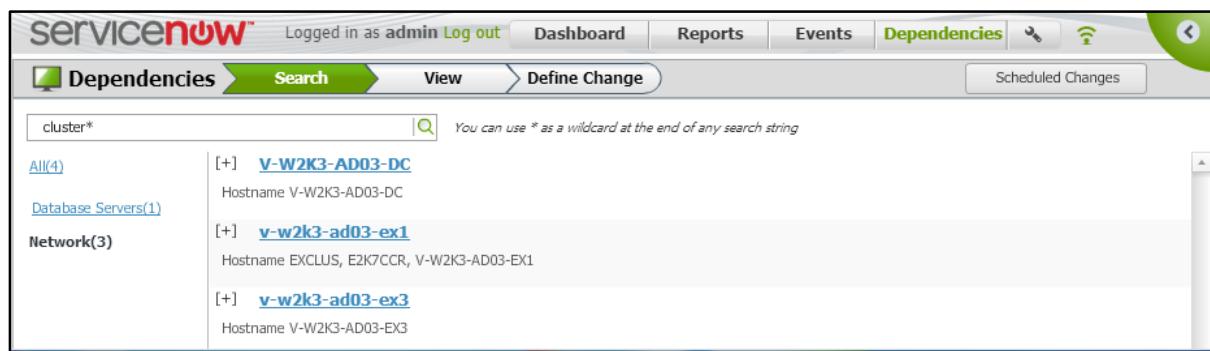


The screenshot shows the ServiceNow Dependencies search interface. The search bar contains "cluster\*". The results pane displays four entries:

- All(4)
  - [+] [Oracle DB:orcl](#) hosted on V-W2K3-32-ORA101  
Instance name orcl
  - [+] [V-W2K3-AD03-DC](#) Hostname V-W2K3-AD03-DC
  - [+] [v-w2k3-ad03-ex1](#) Hostname EXCLUS, E2K7CCR, V-W2K3-AD03-EX1
  - [+] [v-w2k3-ad03-ex3](#) Hostname V-W2K3-AD03-EX3

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



The screenshot shows the ServiceNow Dependencies search interface with the search bar containing "cluster\*". The results pane displays three entries:

- All(4)
  - [+] [V-W2K3-AD03-DC](#) Hostname V-W2K3-AD03-DC
  - [+] [v-w2k3-ad03-ex1](#) Hostname EXCLUS, E2K7CCR, V-W2K3-AD03-EX1
  - [+] [v-w2k3-ad03-ex3](#) Hostname V-W2K3-AD03-EX3

## 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 ...

[-] **IBM WebSphere MQ:QM1** hosted on V-W2K3-32-MQ7    Inner search:  Port  Inclusion    Port searching...

Installation directory C:\Program Files\IBM\WebSphere MQ\  
Queue manager name QM1  
Version 6.0.0.0

[00000010] Intel(R) PRO/1000 MT Network Connection Intel(R) PRO/1000 MT Network Connection (65539)

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

[-] **IBM WebSphere MQ:QM1** hosted on V-W2K3-32-MQ7    Inner search:  Port  Inclusion    Inclusion searching...

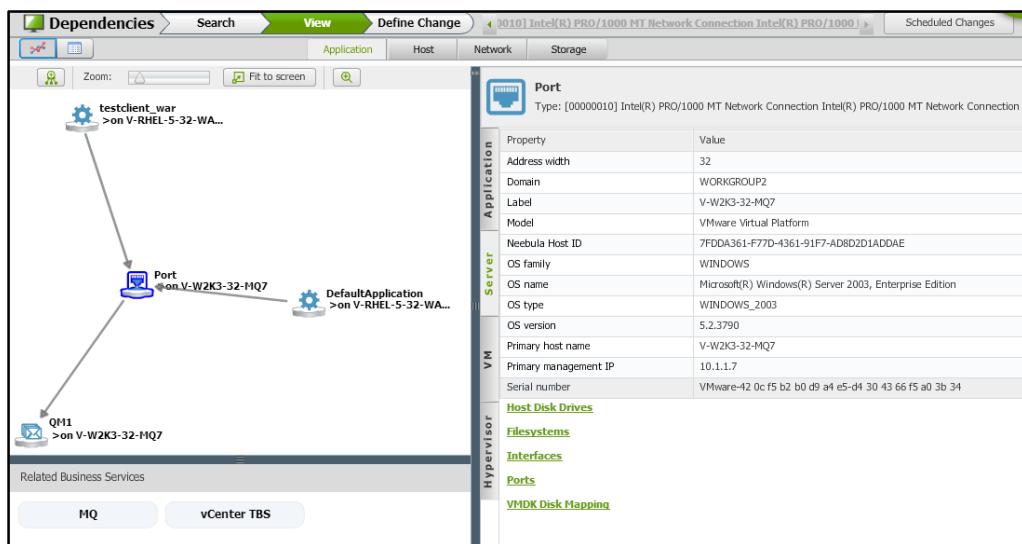
Installation directory C:\Program Files\IBM\WebSphere MQ\  
Queue manager name QM1  
Version 6.0.0.0

BS.REQUEST.ENDPOINT.QUEUE  
BS.RESPONSE.CALLBACKSTATIC1.QUEUE

- **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** panels.

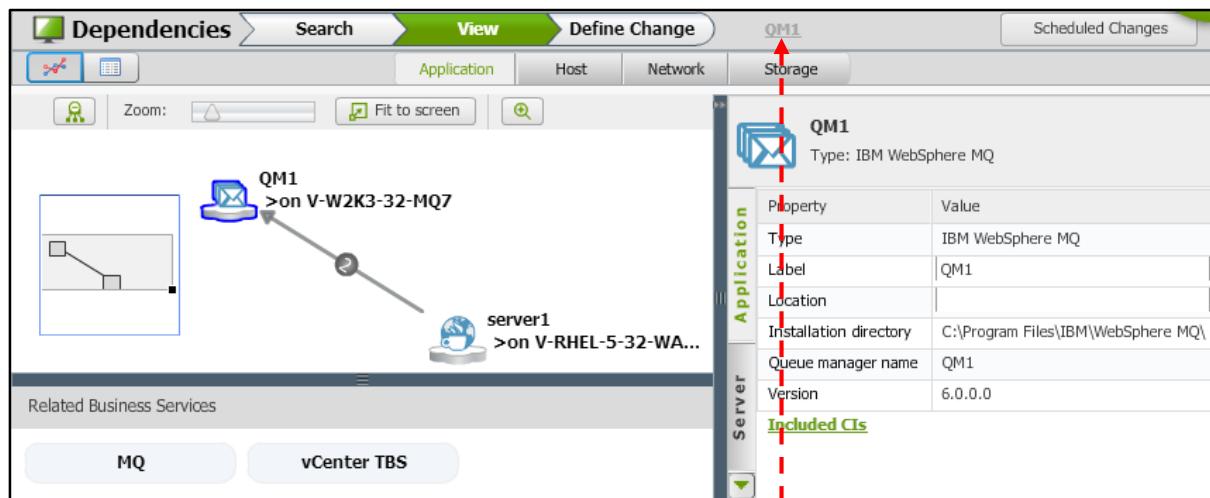
The Dependencies View window displays the CI or the CI's entity map of dependencies. It has 4 panels (**Application**, **Host**, **Network**, **Storage**). Each panel has 3 panes.

- 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.

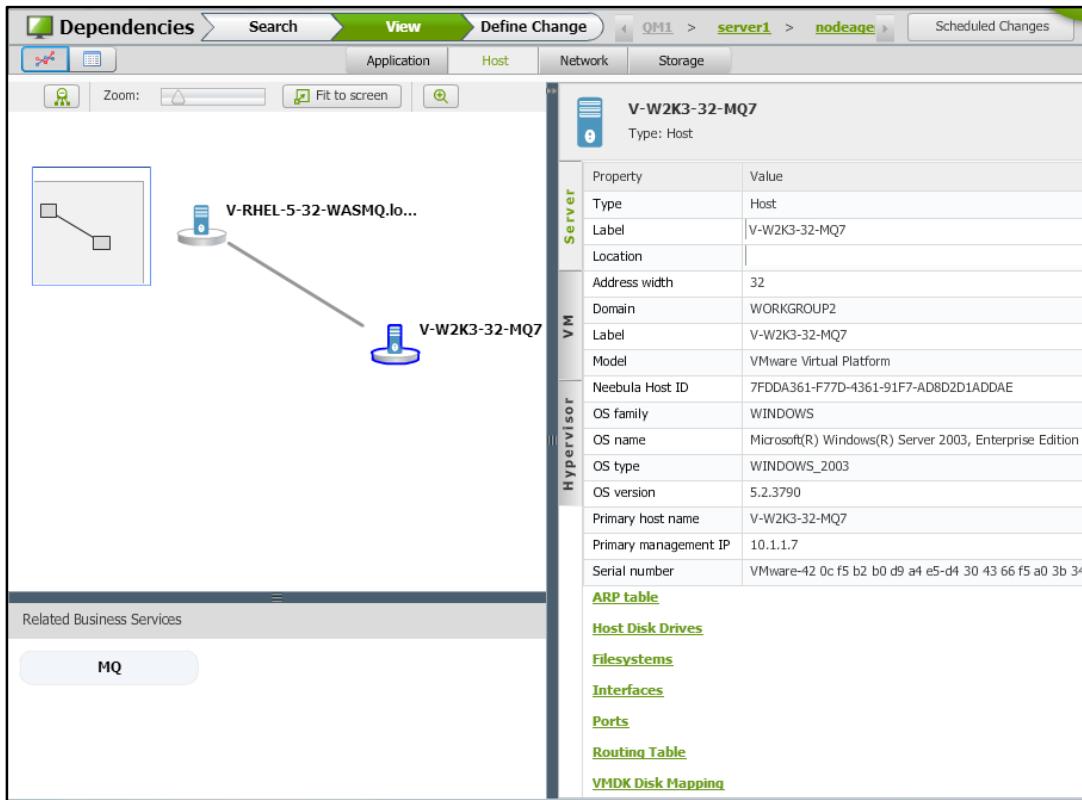
To see the dependencies of any CI that is currently displayed in this window, right-click that CI and select its **Show dependencies** option.



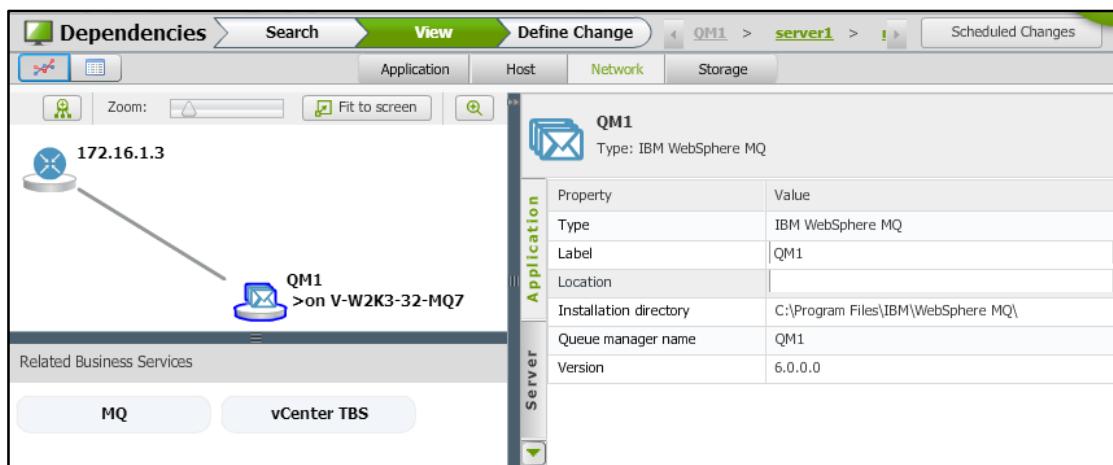
If breadcrumb links for previously displayed CIs do not fit in the top row, scroll-arrows will enable you to click previously displayed links.



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

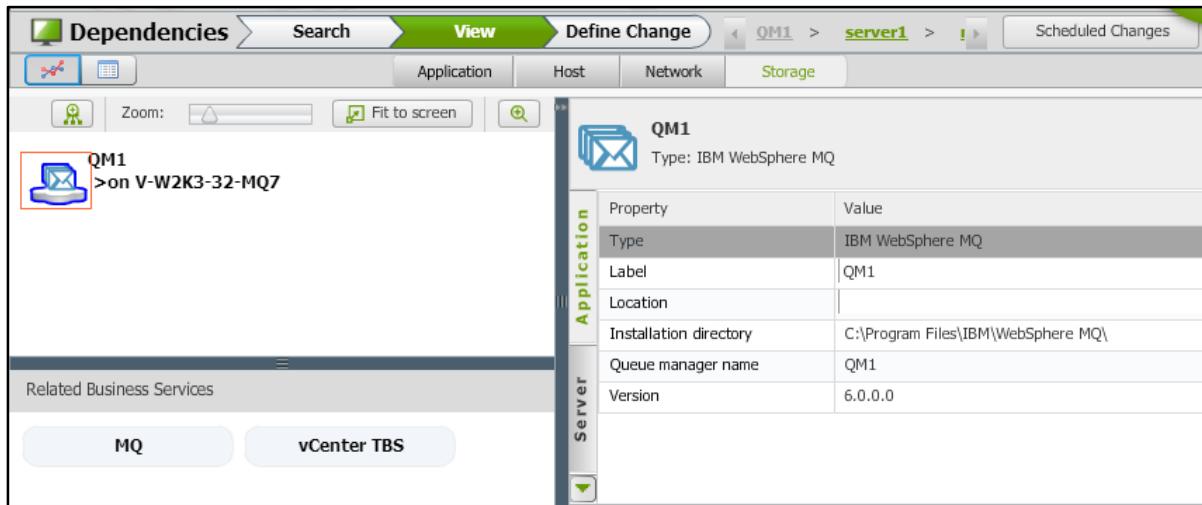
**Figure 38: Dependencies window – Host panel**

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)

The screenshot shows the 'Dependencies' interface with the 'Define Change' tab selected. The 'Add CI to existing scheduled change' radio button is selected. A scheduled change named 'Add more load balancers' is listed with a description 'Add BIG-IP load balancers'. A table titled 'CIs included in this scheduled change:' lists two entries: 'null on 10.1.0.120' and 'null on v-w2k3-sql02-s1.qa.lab.local', both categorized as 'Radware Load Balancer'. An 'Update' button is visible at the bottom right of the table.

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.

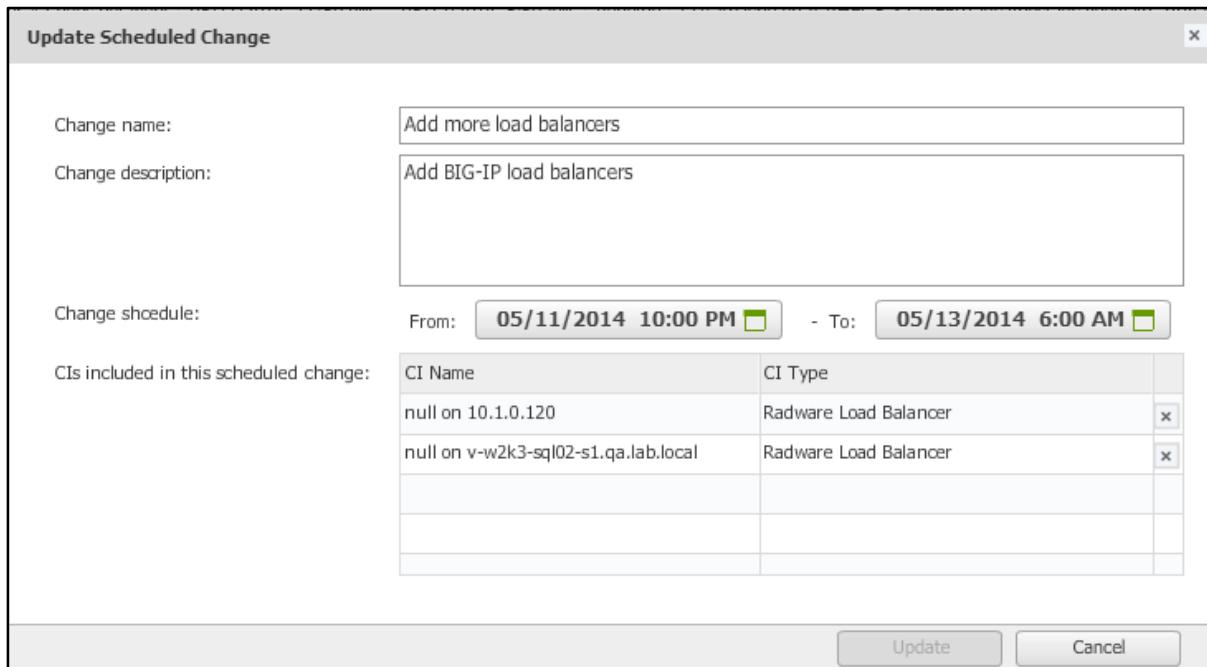
Figure 43: Dependencies window – Scheduled Changes table

The screenshot shows the 'Dependencies' interface with the 'Scheduled Changes' button selected. A table titled 'Scheduled Changes' lists one entry: 'Add more load balancers' with a description 'Add BIG-IP load balancers', status 'Pending', and a note '(2): null on 10.1.0.120, null on v-w2k3-sql02-s1.qa.lab.local'. The 'Actions' column contains edit and delete icons.

## 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

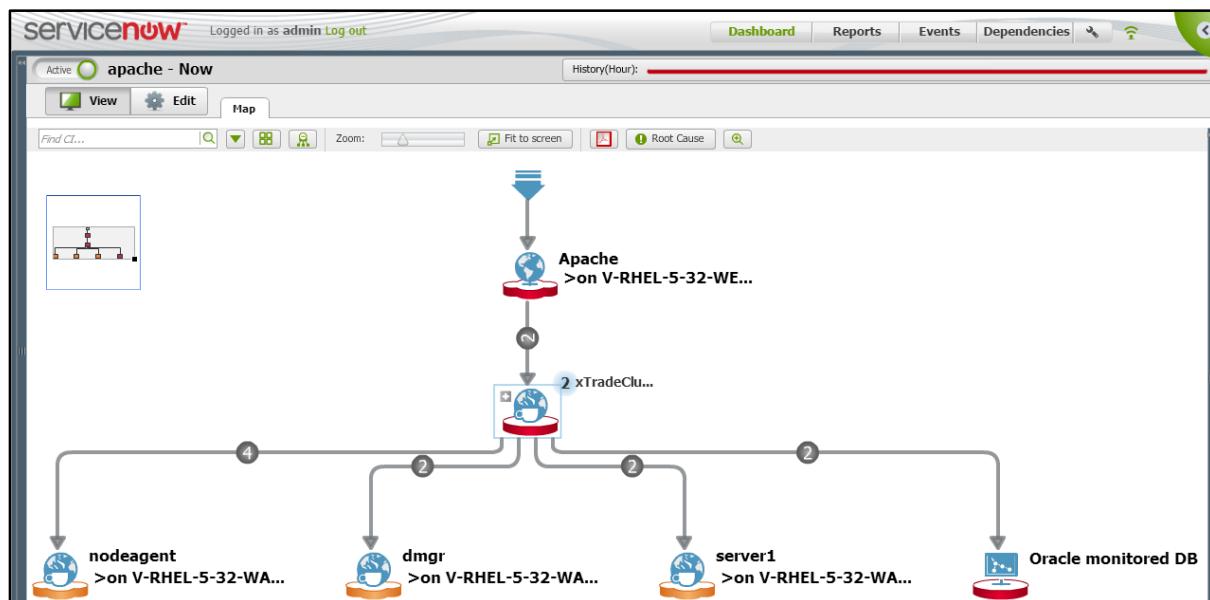
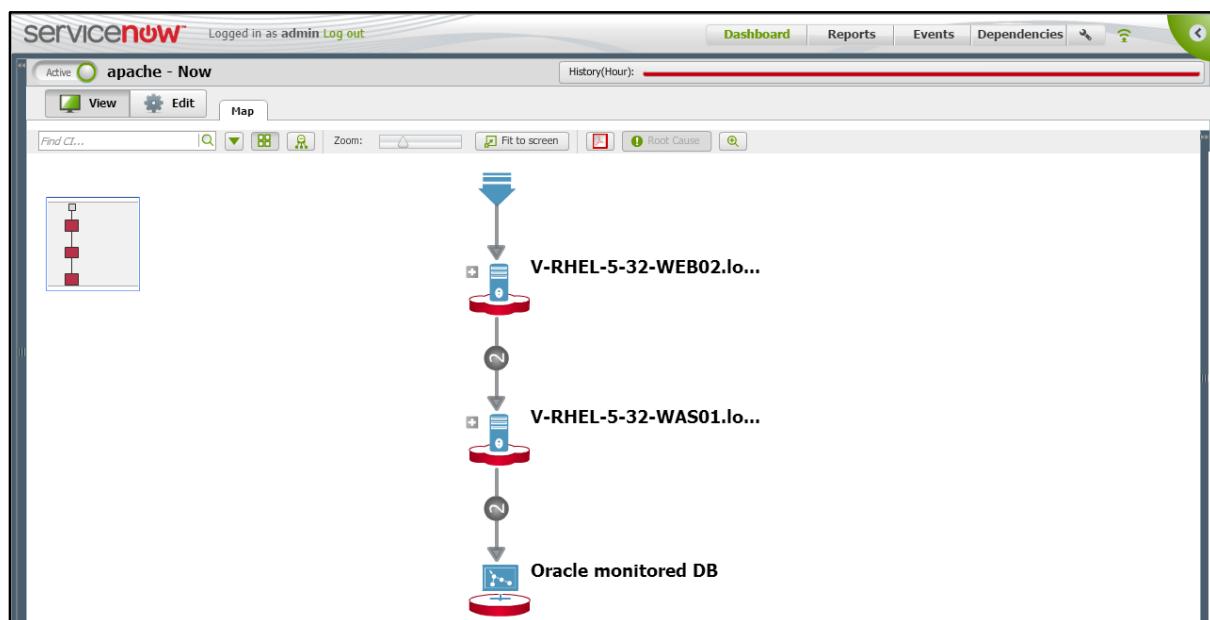


Figure 46: Topology Map with only Hosts displayed



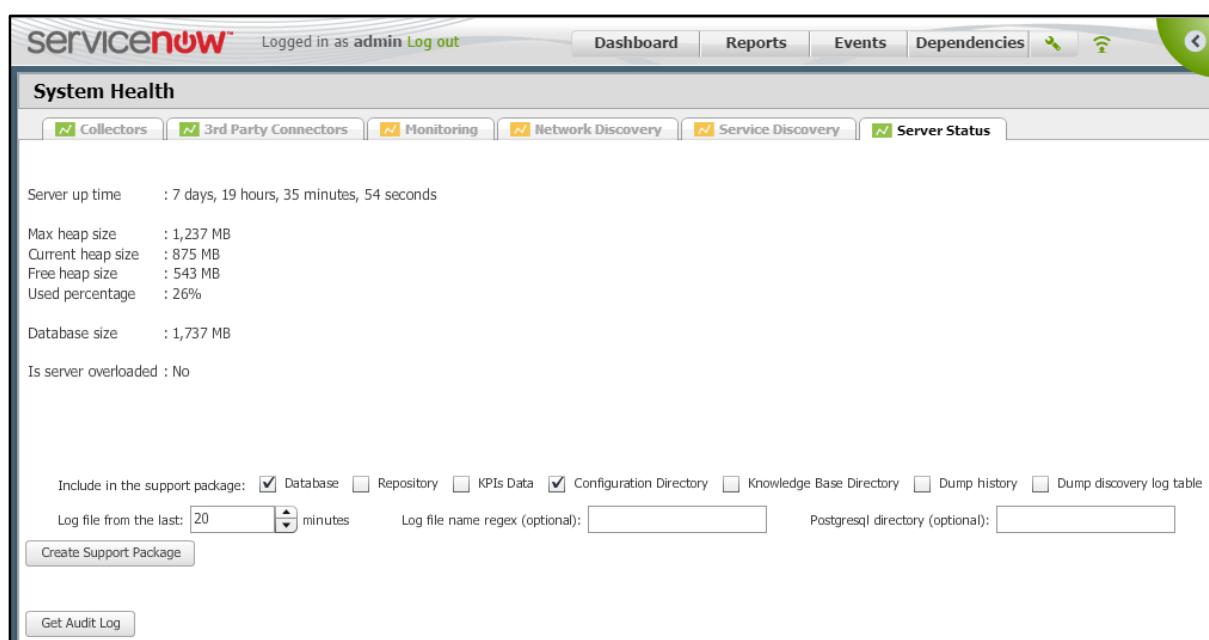
# System Health

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 screenshot shows the ServiceNow System Health screen. At the top, there's a navigation bar with tabs: Dashboard, Reports, Events, Dependencies, and a few others. Below the navigation bar, the title 'System Health' is displayed, followed by a horizontal bar with several tabs: Collectors (green), 3rd Party Connectors (green), Monitoring (yellow), Network Discovery (yellow), Service Discovery (yellow), and Server Status (green). The main content area displays various system statistics:

- Server up time : 7 days, 19 hours, 35 minutes, 54 seconds
- Max heap size : 1,237 MB
- Current heap size : 875 MB
- Free heap size : 543 MB
- Used percentage : 26%
- Database size : 1,737 MB
- Is server overloaded : No

Below these stats, there are several configuration options:

- Include in the support package:  Database  Repository  KPIs Data  Configuration Directory  Knowledge Base Directory  Dump history  Dump discovery log table
- Log file from the last:  minutes Log file name regex (optional):  Postgresql directory (optional):
- Buttons: Create Support Package, Get Audit Log

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  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](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:

Name	Date modified	Type	Size
 SupportPackage_28082014_110603 (1).zip	8/28/2014 11:16 AM	WinRAR ZIP archive	16,917 KB

To view the **Audit Log**, click the  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](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:

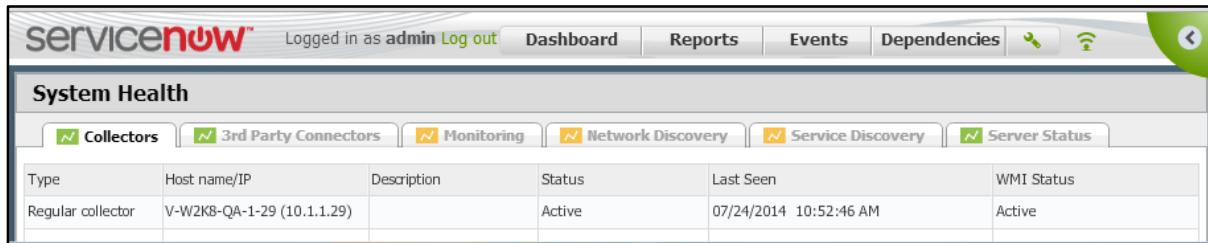
Name	Type	Compressed size	Password protected	Size	Ratio	Date modified
audit.log	Text Document	1 KB	No	8 KB	89%	3/11/2014 4:48 PM

## 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**



The screenshot shows the ServiceNow System Health interface. At the top, there's a navigation bar with tabs for Dashboard, Reports, Events, Dependencies, and a search/filter icon. Below the navigation bar is a sub-header "System Health". Underneath is a table titled "Collectors". The table has columns for Type, Host name/IP, Description, Status, Last Seen, and WMI Status. One row is visible, showing a "Regular collector" named "V-W2K8-QA-1-29 (10.1.1.29)" with an "Active" status, last seen at "07/24/2014 10:52:46 AM", and an "Active" WMI status. Above the table, there are several status indicators: Collectors (green), 3rd Party Connectors (green), Monitoring (yellow), Network Discovery (yellow), Service Discovery (yellow), and Server Status (green).

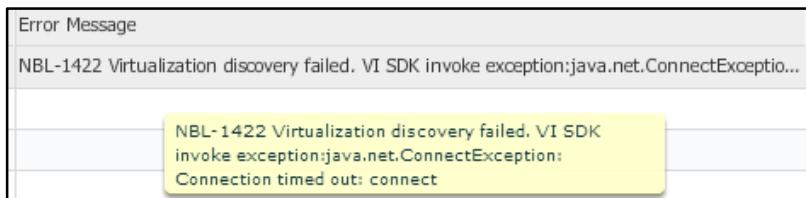
## 3<sup>rd</sup> Party Connectors panel

This panel displays the health status of each 3<sup>rd</sup> Party Connector. Click the **3<sup>rd</sup> 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 – 3<sup>rd</sup> Party Connectors panel**

Type	Host name/IP	Status	Error Message	Last Run	Frequency(min.)	Actions
VMware vCenter	172.16.1.45	Active		04/10/2014 7:14:54 AM	1440	
VMware vCenter	172.16.1.13	Inactive	NBL-1422 Virtualization discovery failed. VI SDK invoke exception:java.net.ConnectException: Connection timed out: connect	04/07/2014 7:53:25 AM	660	

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 3<sup>rd</sup> Party Connector** message is displayed.

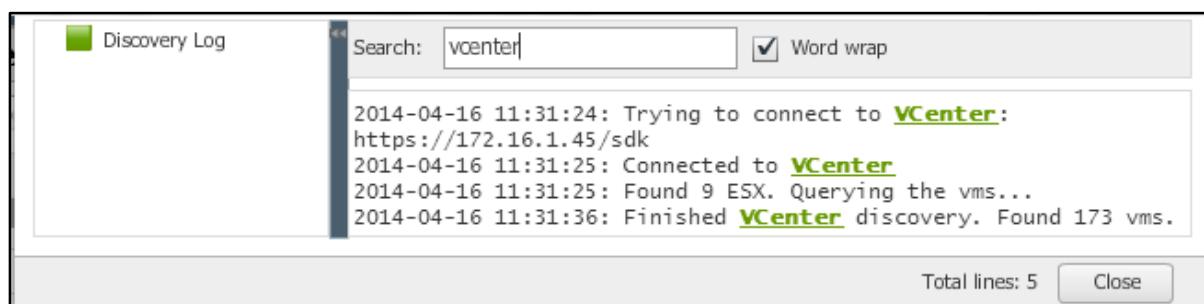


Click the **Show discovery log** button to display the log contents. The log contains a trace of all 3<sup>rd</sup> party connector activity and is used by ServiceWatch Customer Support to diagnose problems.

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: 3<sup>rd</sup> Party Connectors – Discovery Log window**

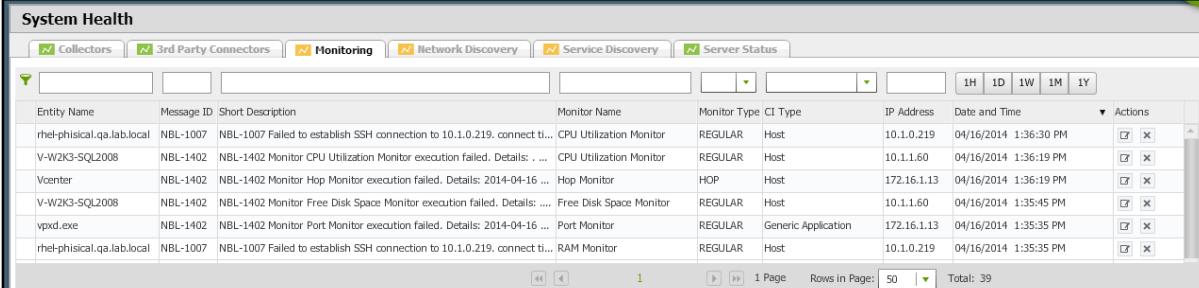


Click to close the **Discovery Log** window.

## 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.

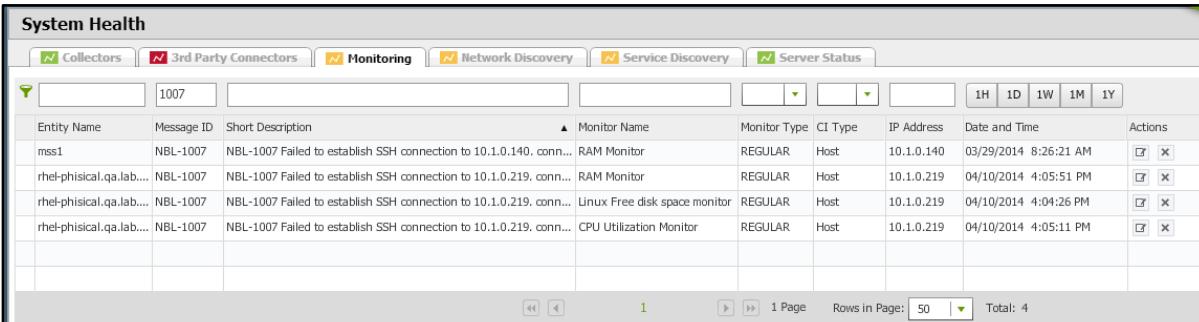
**Figure 51: System Health screen – Monitoring panel**



System Health							
Collectors		3rd Party Connectors		Monitoring		Network Discovery	
Entity Name	Message ID	Short Description	Monitor Name	Monitor Type	CI Type	IP Address	Date and Time
rhel-physical.qa.lab.local	NBL-1007	NBL-1007 Failed to establish SSH connection to 10.1.0.219. connect ti...	CPU Utilization Monitor	REGULAR	Host	10.1.0.219	04/16/2014 1:36:30 PM
V-W2K3-SQL2008	NBL-1402	NBL-1402 Monitor CPU Utilization Monitor execution failed. Details: ...	CPU Utilization Monitor	REGULAR	Host	10.1.1.60	04/16/2014 1:36:19 PM
voenter	NBL-1402	NBL-1402 Monitor Hop Monitor execution failed. Details: 2014-04-16 ...	Hop Monitor	HOP	Host	172.16.1.13	04/16/2014 1:36:19 PM
V-W2K3-SQL2008	NBL-1402	NBL-1402 Monitor Free Disk Space Monitor execution failed. Details: ...	Free Disk Space Monitor	REGULAR	Host	10.1.1.60	04/16/2014 1:35:45 PM
vpxd.exe	NBL-1402	NBL-1402 Monitor Port Monitor execution failed. Details: 2014-04-16 ...	Port Monitor	REGULAR	Generic Application	172.16.1.13	04/16/2014 1:35:35 PM
rhel-physical.qa.lab.local	NBL-1007	NBL-1007 Failed to establish SSH connection to 10.1.0.219. connect ti...	RAM Monitor	REGULAR	Host	10.1.0.219	04/16/2014 1:35:35 PM

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 see only messages whose **Message ID** contains 1007:

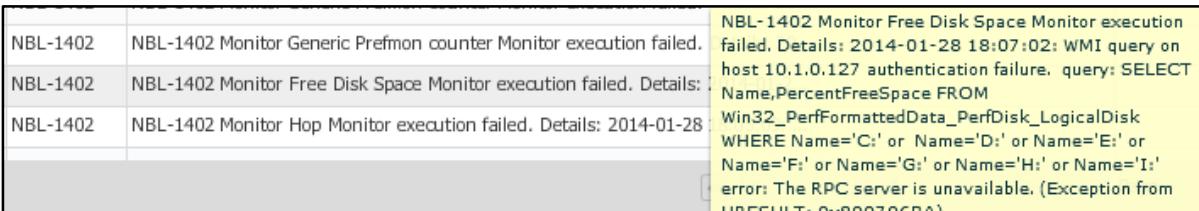
**Figure 52: System Health screen – Monitoring panel filtered by Message ID**



System Health							
Collectors		3rd Party Connectors		Monitoring		Network Discovery	
Entity Name	Message ID	Short Description	Monitor Name	Monitor Type	CI Type	IP Address	Date and Time
mss1	NBL-1007	NBL-1007 Failed to establish SSH connection to 10.1.0.140. conn...	RAM Monitor	REGULAR	Host	10.1.0.140	03/29/2014 8:26:21 AM
rhel-physical.qa.lab....	NBL-1007	NBL-1007 Failed to establish SSH connection to 10.1.0.219. conn...	RAM Monitor	REGULAR	Host	10.1.0.219	04/10/2014 4:05:51 PM
rhel-physical.qa.lab....	NBL-1007	NBL-1007 Failed to establish SSH connection to 10.1.0.219. conn...	Linux Free disk space monitor	REGULAR	Host	10.1.0.219	04/10/2014 4:04:26 PM
rhel-physical.qa.lab....	NBL-1007	NBL-1007 Failed to establish SSH connection to 10.1.0.219. conn...	CPU Utilization Monitor	REGULAR	Host	10.1.0.219	04/10/2014 4:05:11 PM

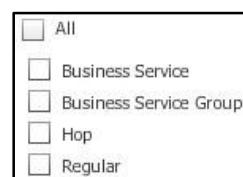
If the cursor hovers over a **Short Description** text, the full description is displayed in a tooltip. For example:

**Figure 53: Full Description in a tool tip**



NBL-1402	NBL-1402 Monitor Generic Prefmon counter Monitor execution failed.	NBL-1402 Monitor Free Disk Space Monitor execution failed. Details: 2014-01-28 18:07:02: WMI query on host 10.1.0.127 authentication failure. query: SELECT Name,PercentFreeSpace FROM Win32_PerfFormattedData_PerfDisk_LogicalDisk WHERE Name='C:' or Name='D:' or Name='E:' or Name='F:' or Name='G:' or Name='H:' or Name='I:' error: The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)
NBL-1402	NBL-1402 Monitor Free Disk Space Monitor execution failed. Details: ...	
NBL-1402	NBL-1402 Monitor Hop Monitor execution failed. Details: 2014-01-28	

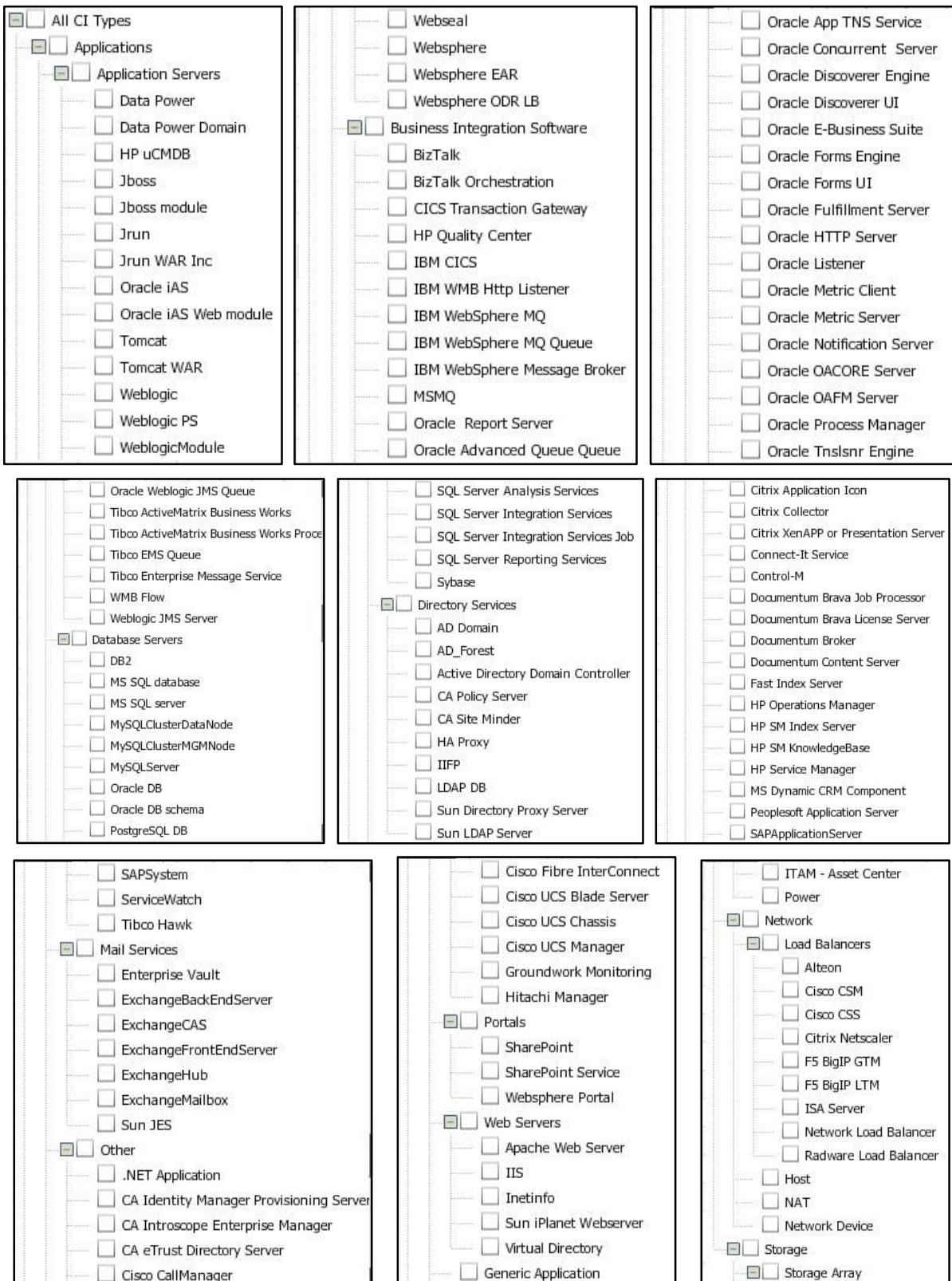
To filter messages by **Monitor Type**, click the down-arrow above the header and select the desired options in the drop-down menu.



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**



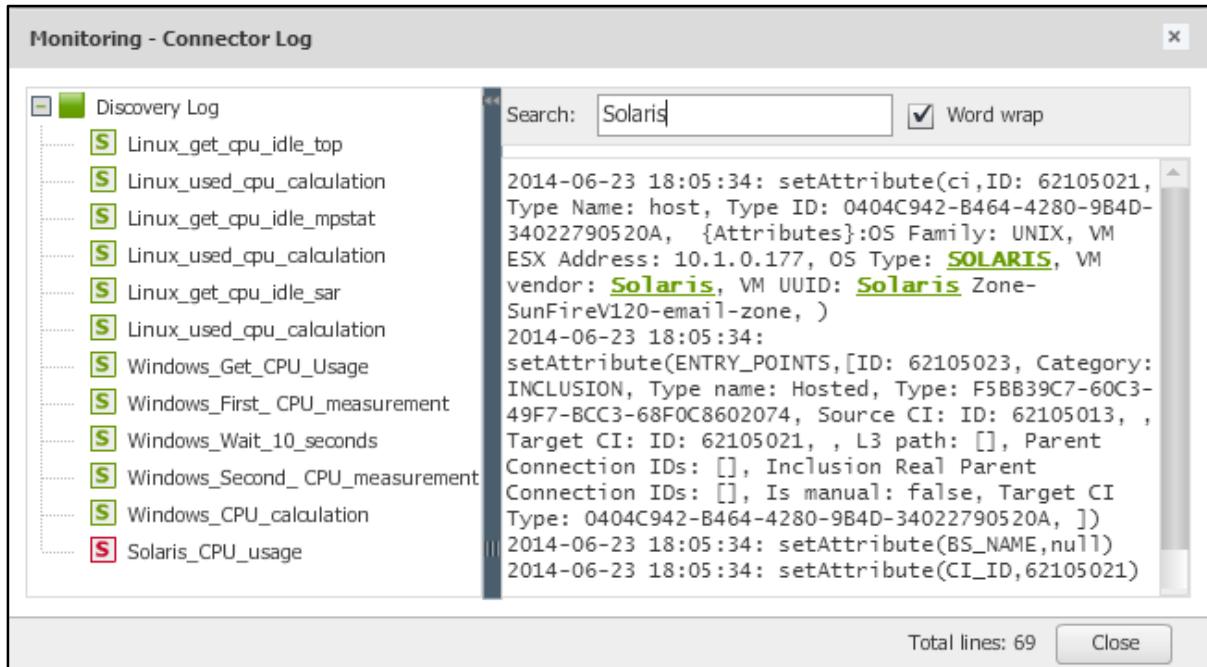
## Actions column

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

Message Type	Message ID	Short Description	Source	IP Address	Date and Time	Actions
Host Detection	NBL-1363	NBL-1363 Host 192.168.100.253 is not reachable by SSH/WMI/SNMP but answers to ping. Please check con...	ARP Scan - Network Device	192.168.100.253	04/09/2014 4:38:48 PM	<input type="checkbox"/> <input checked="" type="checkbox"/>
Host Detection	NBL-1364	NBL-1364 Host 10.10.0.1 is not reachable by SSH/WMI/SNMP and does not reply to ping. Please check con...	Router Scan	10.10.0.1	04/09/2014 3:47:03 PM	<input type="checkbox"/> <input checked="" type="checkbox"/>
Host Detection	NBL-1055	NBL-1055 All ports closed on host 10.0.1.109. Host might be down or unreachable.	ARP Scan - Network Device	10.0.1.109	04/09/2014 1:32:20 PM	<input type="checkbox"/> <input checked="" type="checkbox"/>
Host Detection	NBL-1364	NBL-1364 Host 4.0.0.1 is not reachable by SSH/WMI/SNMP and does not reply to ping. Please check con...	Router Scan	4.0.0.1	04/09/2014 9:31:16 AM	<input type="checkbox"/> <input checked="" type="checkbox"/>
Host Detection	NBL-1055	NBL-1055 All ports closed on host 10.0.1.112. Host might be down or unreachable.	ARP Scan - Network Device	10.0.1.112	04/09/2014 8:34:09 AM	<input type="checkbox"/> <input checked="" type="checkbox"/>
Host Detection	NBL-1364	NBL-1364 Host 10.10.0.198 is not reachable by SSH/WMI/SNMP and does not reply to ping. Please check co...	Router Scan	10.10.0.198	04/09/2014 5:57:37 AM	<input type="checkbox"/> <input checked="" type="checkbox"/>

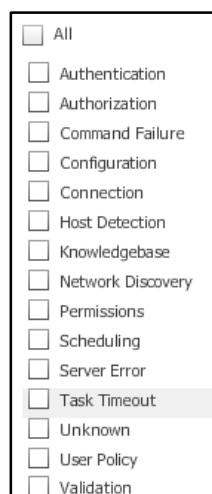
Type a string in any of the text boxes above each column and click **Enter** or ↵ to display only data that matches that string. There are no wildcards. Records are displayed if the trimmed search string occurs anywhere in the field. For example, to see only messages whose **Message ID** contains 1005:

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

Message Type	Message ID	Short Description	Source	IP Address	Date and Time	Actions
Authentication	NBL-1005	NBL-1005 SSH authentication failed on host 50.17.189.50	Router Scan	50.17.189.50	03/21/2014 5:52:28 AM	<input type="checkbox"/> <input checked="" type="checkbox"/>

Click one of the **1H**, **1D**, **1W**, **1M**, or **1Y** 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.

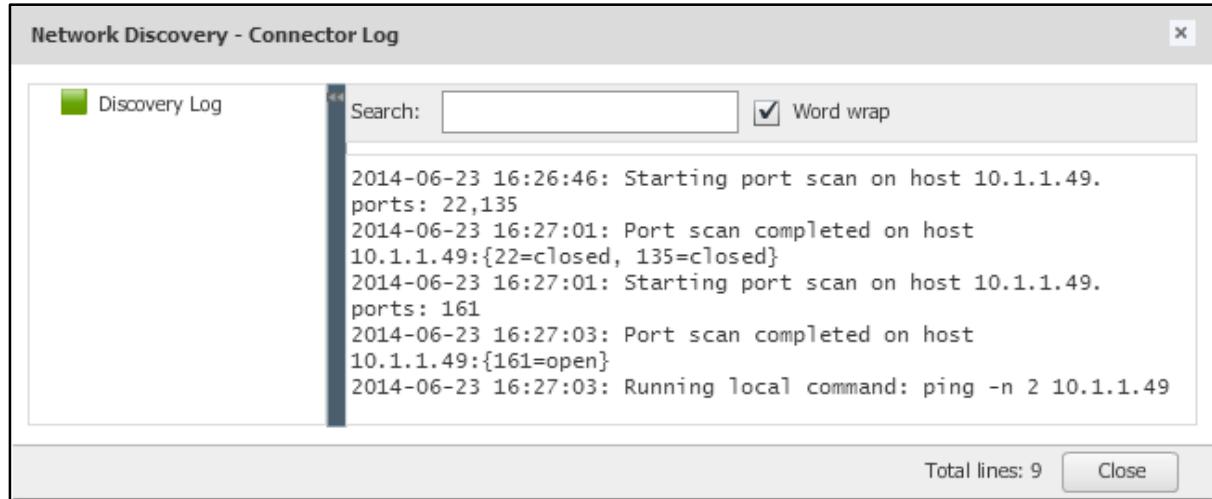


If the cursor hovers over a **Short Description** text, the full description is displayed in a tooltip. For example:

**Figure 58: Full Description in a tool tip**

Host Detection	NBL-1363	NBL-1363 Host 50.95.22.1 is not reachable by SSH/WMI/SNMP but answers to ping. Please check connectivity fro...
Host Detection	NBL-1364	NBL-1364 Host 192.168.2.1 is not reachable by SSH/WM
Host Detection	NBL-1364	NBL-1364 Host 4.0.0.1 is not reachable by SSH/WMI/SN
Host Detection	NBL-1364	NBL-1364 Host 10.1.4.2 is not reachable by SSH/WMI/SN

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.

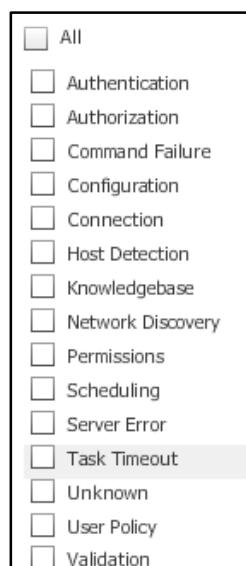
**Figure 60: System Health screen – Service Discovery panel**

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 see only messages whose **Message ID** contains 1077:

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

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 **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**

Business Service Name	Category	Message ID	Short Description	
Accounts test	Permissions	NBL-1436	NBL-1436 Permission issues: Command: type c:\ExchangeSetupLogs\ExchangeSetup.log   findstr /I ExchangeLegacyDN. Response:	
Accounts test	Permissions	NBL-1436	NBL-1436 Permission issues: Command: type c:\ExchangeSetupLogs\ExchangeSetup.log   findstr /I ExchangeLegacyDN. Response:	
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	NBL-1436 Permission issues: Command: type c:\ExchangeSetupLogs\ExchangeSetup.log   findstr /I ExchangeLegacyDN. Response:
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	Command: type
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	d:\ExchangeSetupLogs\ExchangeSetup.log   findstr /I ExchangeLegacyDN. Response:
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	Command: type
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	c:\ExchangeSetupLogs\ExchangeSetup.log   findstr "Used domain controller". Response:
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	Command: type
	Host Detection	NBL-1129	NBL-1129 VM is down (powered off/suspended/deleted)	d:\ExchangeSetupLogs\ExchangeSetup.log   findstr "Used domain controller". Response:

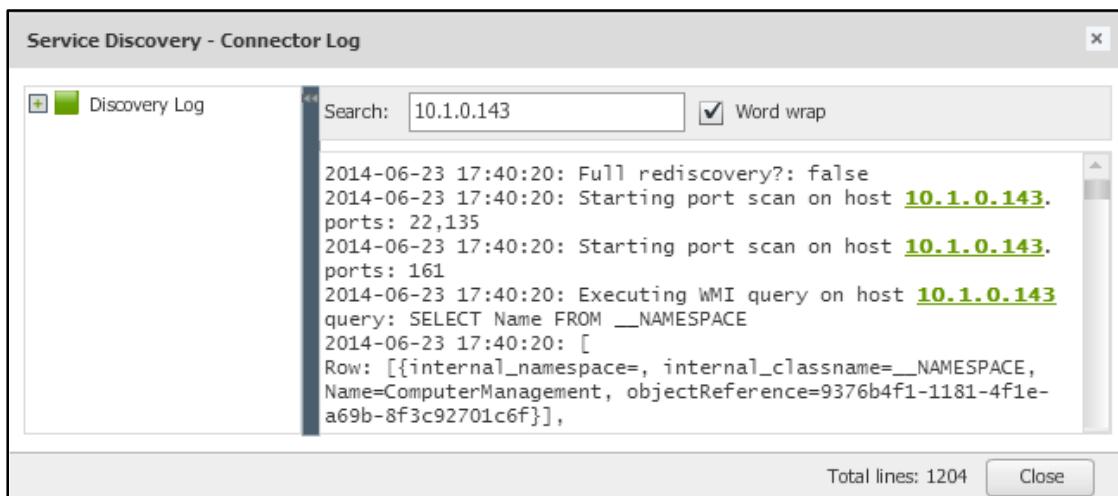
### ***Actions column***

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  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



The screenshot shows the 'Settings' menu interface. At the top left is a gear icon. The menu is divided into several sections:

- Knowledge Base**:
  - > CI Types, Patterns & Monitors Definitions
  - > Entry Point Types
  - > Event Sources/Rules
  - > Group & Business Service Monitors
  - > Import / Export
- General**:
  - > Global Parameters
  - > License Information
- User Management**:
  - > Roles
  - > Users
- System**:
  - > Alerts
  - > Collectors
  - > Credentials
  - > Infrastructure Monitoring
  - > Monitoring Connectors
  - > Network Discovery
  - > System Health
  - > Virtualization Connectors

# 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).

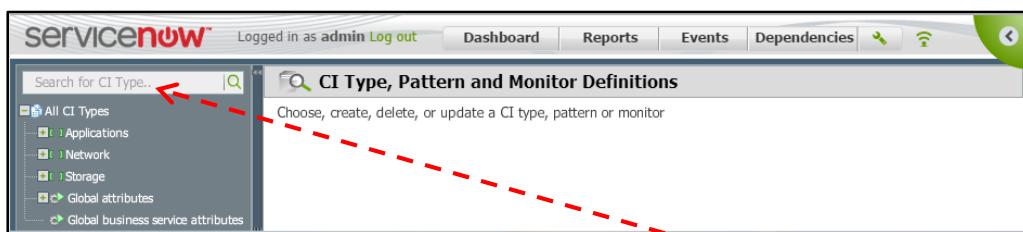
## System

- [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 3<sup>rd</sup> 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 (page 127).
- [SYSTEM HEALTH](#) – Display discovery messages about Collectors, 3<sup>rd</sup> 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 127).

# 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
<ul style="list-style-type: none"> <li>▪ Application Server</li> <li>▪ Business Integration Software</li> <li>▪ Database Server</li> <li>▪ Directory Services</li> <li>▪ Enterprise Applications</li> <li>▪ Mail Services</li> <li>▪ Other</li> <li>▪ Portals</li> <li>▪ Web Servers</li> <li>▪ Generic Application</li> <li>▪ ITAM - Asset Center</li> <li>▪ Load Balancers</li> </ul>	<ul style="list-style-type: none"> <li>▪ Clone CI Type</li> <li>▪ Add New Pattern</li> <li>▪ Add New Monitor</li> <li>▪ Add New Quick Monitor</li> </ul>	<ul style="list-style-type: none"> <li>▪ Delete Pattern</li> <li>▪ Copy Pattern</li> </ul>
▪ Web Server monitors	<ul style="list-style-type: none"> <li>▪ Clone CI Type</li> <li>▪ Add New Pattern</li> <li>▪ Add New Monitor</li> <li>▪ Add New Quick Monitor</li> </ul>	<ul style="list-style-type: none"> <li>▪ Delete Monitor</li> <li>▪ Copy Monitor</li> </ul>
▪	▪	▪
<ul style="list-style-type: none"> <li>▪ NAT (Network Address Translation)</li> <li>▪ Network Device</li> <li>▪ Storage</li> </ul>	<ul style="list-style-type: none"> <li>▪ Add New Monitor</li> <li>▪ Add New Quick Monitor</li> </ul>	

## 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.

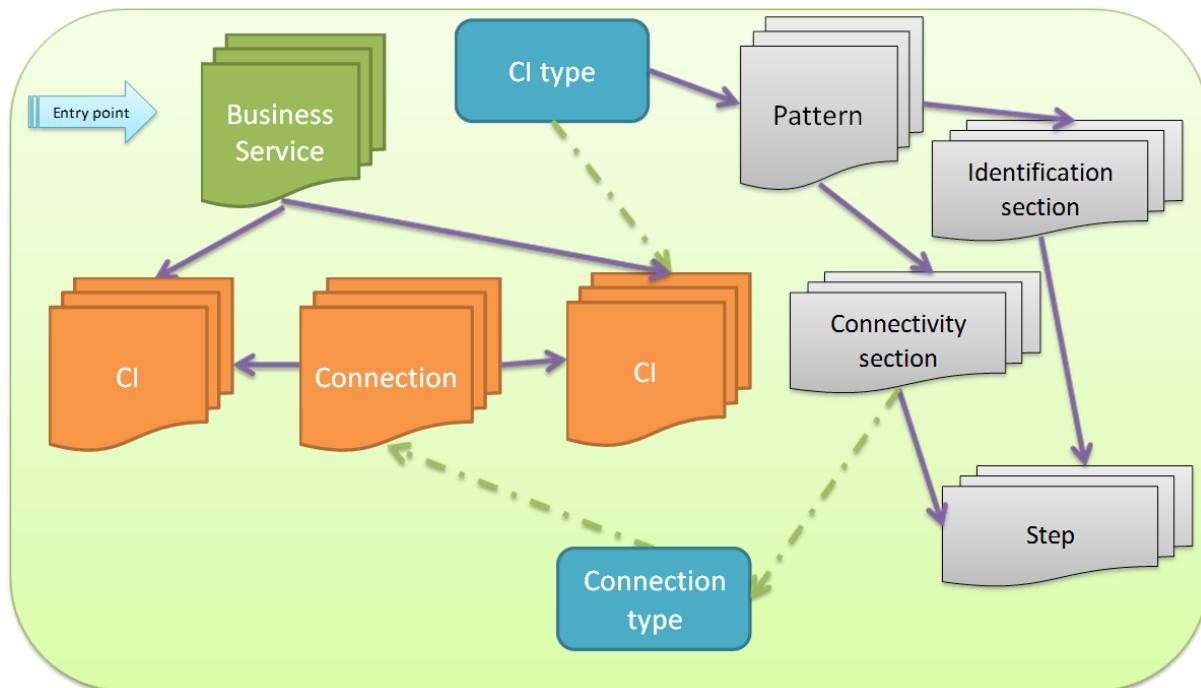
Defining discovery patterns for a CI type is a 2-part process:

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

The screenshot shows the 'CI Type Definition' window in ServiceNow. On the left is a navigation tree with categories like HPOM Events Integration, HP Operations Manager for Windows, HP SM Index Server, etc. The 'Enterprise Vault' node under 'Mail Services' is selected. The main panel has fields for 'CI Type name' (Enterprise Vault), 'Display name' (Enterprise Vault), 'Description' (Enterprise Vault), 'Icon' (a globe icon with an envelope), 'Parent CI Type' (empty), and 'Scheduling' (Normal). Below this is a table titled 'CI Attributes' with columns for Name, Description, Display Name, Type, Key, Required, Editable, and Searchable. Rows include 'InstallDir' (String, Required, Editable), 'SiteID' (String, Required), 'alternate\_label' (String, Editable, Searchable), 'app\_processes' (Table, Editable), 'app\_services' (Table, Editable), 'extended\_attr' (Table, Editable), 'label' (Label, Editable, Searchable), 'location' (String, Required, Editable), 'name' (String, Editable), 'processes\_with\_creation\_time' (Table, Editable), 'tracked\_files' (Table, Editable), and 'version' (String, Required, Editable). A dropdown menu in the 'Type' column for 'version' is open, showing options: String, Table, Boolean, Numeric, and String. At the bottom are 'Delete' and 'Save' buttons.

**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

The screenshot shows the 'Table Attributes' window. It has a table with columns 'Name', 'Description', and 'Type'. Rows include 'file\_path' (String), 'last\_modification' (String), 'owner' (String), 'checksum' (String), 'content' (String), and 'revision' (String). At the bottom are 'OK' and 'Cancel' buttons.

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.

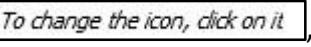
If you click the icon next to the text  *To change the icon, click on it*, the **Choose an Icon** window is displayed. Select the icon that best identifies the component.

Figure 69: Choose an icon window



After creating or modifying the CI Type data, click .

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  near the bottom right corner of the **CI Type Definition – Draft CI Type** screen.

Figure 70: CI Type Definition – Draft CI Type screen

Name	Description	Display Name	Type	Key	Required	Editable	Searchable
alternate_label	GUI alternate display label	Label	String			✓	
app_processes		Application Processes	Table			✓	
app_services		Application Services	Table			✓	
extended_attr		Extended Attributes	Table			✓	
label	GUI display label	Label	String			✓	
location		Location	String			✓	
processes_with_creation_time		Processes with creation time	Table			✓	
tracked_files		Tracked Files	Table			✓	

## 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

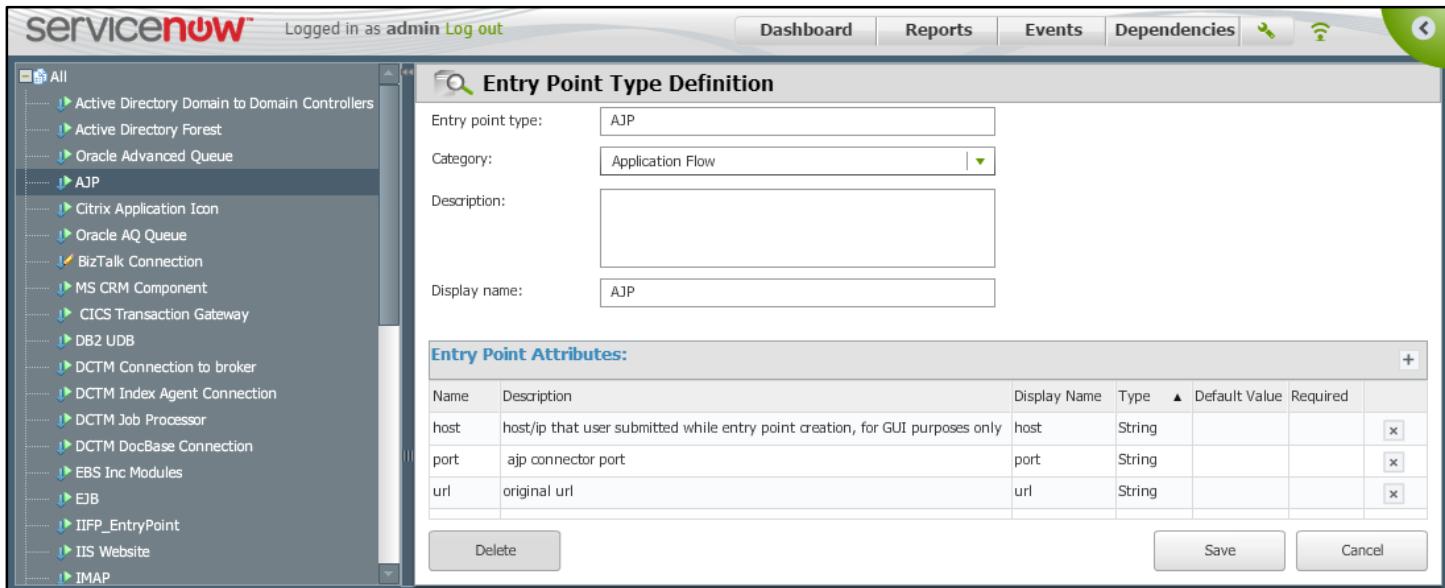
The screenshot shows the ServiceNow interface for creating a new monitor. The left sidebar lists various Configuration Item (CI) types, with 'Host' selected. The main window title is 'Quick Monitor 08/28/2014 12:02 PM'. The 'Definition' section includes fields for Name (set to 'Quick Monitor 08/28/2014 12:02 PM'), Associate with (set to 'host'), Description (empty), and Units (empty). The 'Scheduling' section allows setting the monitoring frequency ('Run monitor every: 10 Minutes') and the days ('Run at: Every day, Sunday through Saturday'). The 'Monitor type' section lets you choose the target machines ('All machines' is selected) and the monitoring type ('Please select type...'). Buttons at the bottom include 'Debug', 'Test', 'Create', and 'Cancel'.

## Entry Point Types

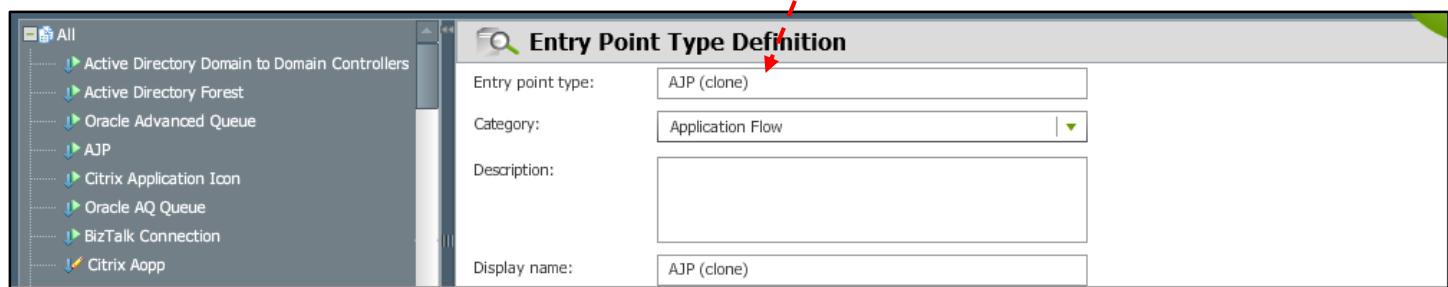
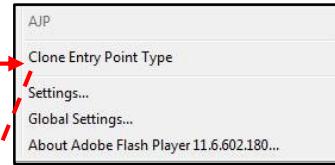
Click the **Entry Point Types** link in the **Settings** menu (Figure 64).

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

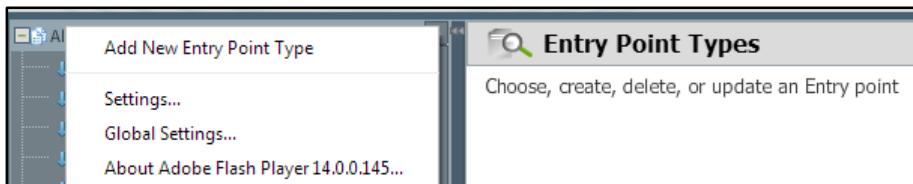
Figure 75: Displaying an Entry Point Type



- 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

Name	Description	Display Name	Type	Default Value	Required
host	host/ip that user submitted while entry point creation, for GUI purposes only	Host	String		<input checked="" type="checkbox"/>
port		Port	Numeric	80	<input checked="" type="checkbox"/>
protocol	http or https	Protocol	String	http	<input checked="" type="checkbox"/>
url	URL of the entry point	URL	String		<input checked="" type="checkbox"/>

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](#)

The screenshot shows the ServiceNow interface with the 'Events' module selected. The top navigation bar includes 'Logged in as admin Log out', 'Dashboard', 'Reports', 'Events', 'Dependencies', and icons for search, refresh, and help. The main content area has a title 'Events' with a warning icon. A sidebar on the left contains a search bar and a tree view labeled 'Event Rules by Sources' with nodes like 'enterprises.20006.1.5' and 'enterprises.20006.1.7'. The main pane below the title contains the text: 'Choose an event binding rule from the tree, or click on a new binding rule button to define a new one'.

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 , an empty **Event Source Definition** screen is displayed.

[Figure 78: Event Source Definition screen](#)

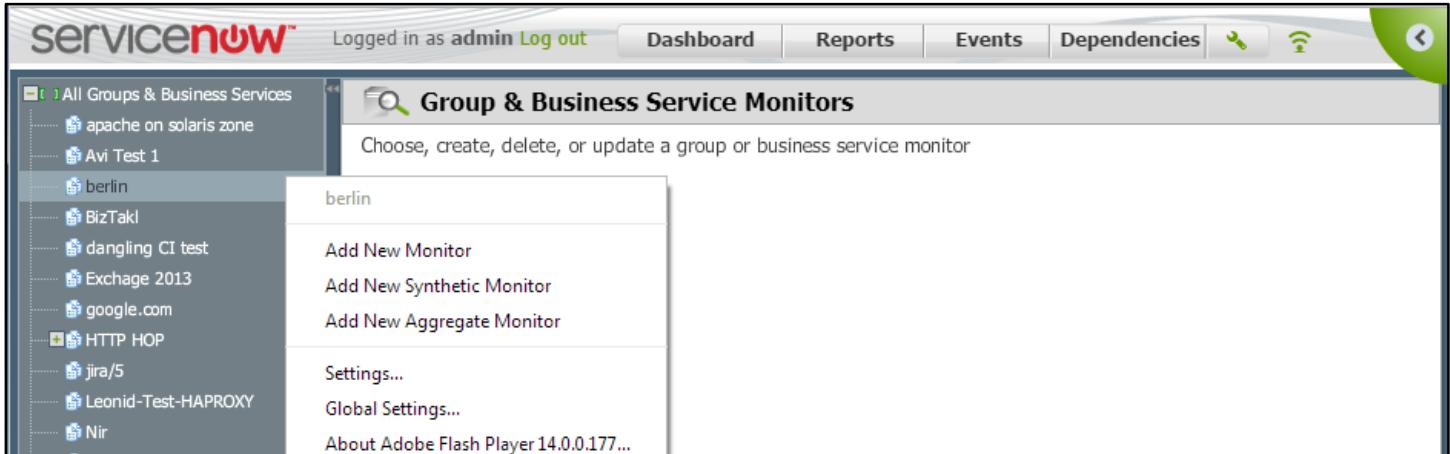
The screenshot shows the 'Event Source Definition' screen. The top navigation bar is identical to Figure 77. The main content area has a title 'Event Source Definition'. On the left is a sidebar with a search bar and a tree view of event sources, including 'enterprises.20006.1.5', 'enterprises.20006.1.7', 'hpom', 'HPOMWIN', 'kuku', 'mom', 'netappDataFabricManager', 'oraEM4Traps', 'snmpTraps', 'SolarWinds', 'Splunk', 'vmwVC', 'vtpNotifications', and 'whatsup'. The main pane contains two tables: 'Fields Mapping' and 'Constant Mappings'. The 'Fields Mapping' table has columns 'Source Field', 'Target Field', and 'Translation'. The 'Constant Mappings' table has columns 'Target Field' and 'Value'.

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.

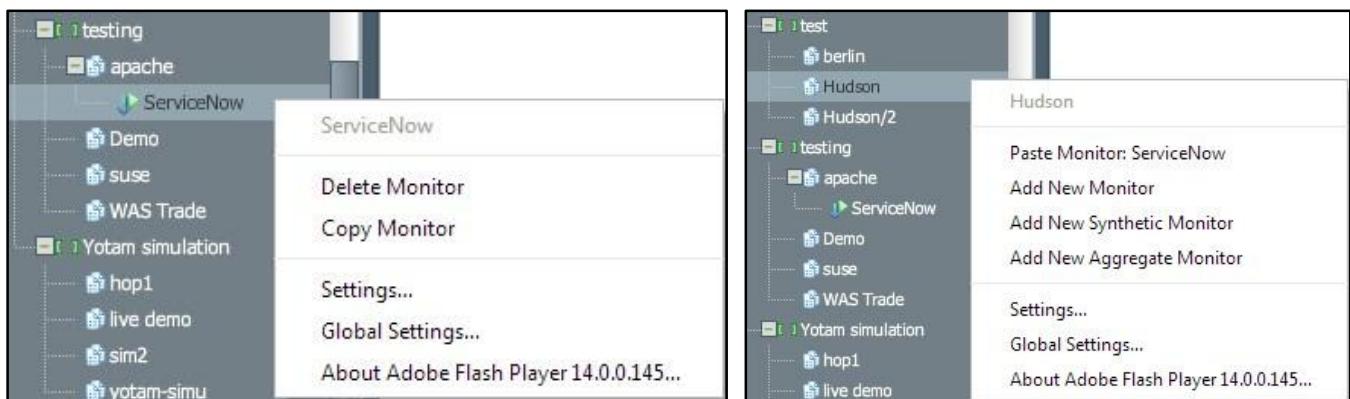
Figure 79: Group & Business Service Monitors window



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

The screenshot displays the 'Definition' page of a Business Service Monitor in ServiceNow. The left sidebar lists various business services and groups. The main area contains several configuration sections:

- Definition:** Fields for Name, Description, and Units, with a checked checkbox for 'Enable monitor'.
- Scheduling:** Set to run every 10 minutes, every day, on all days of the week.
- Parameters:** A table titled 'Monitor Parameters' with columns for Parameter Name and Value.
- Use metric:** Options for Support delta, thresholds (Warning, Minor, Major, Critical), and a radio button for Scalar attribute.
- Use condition:** A severity dropdown set to Critical, a search bar containing 'Contains', and an event message input field.

At the bottom are buttons for Delete, Monitor Steps, Save, and Check Monitor.

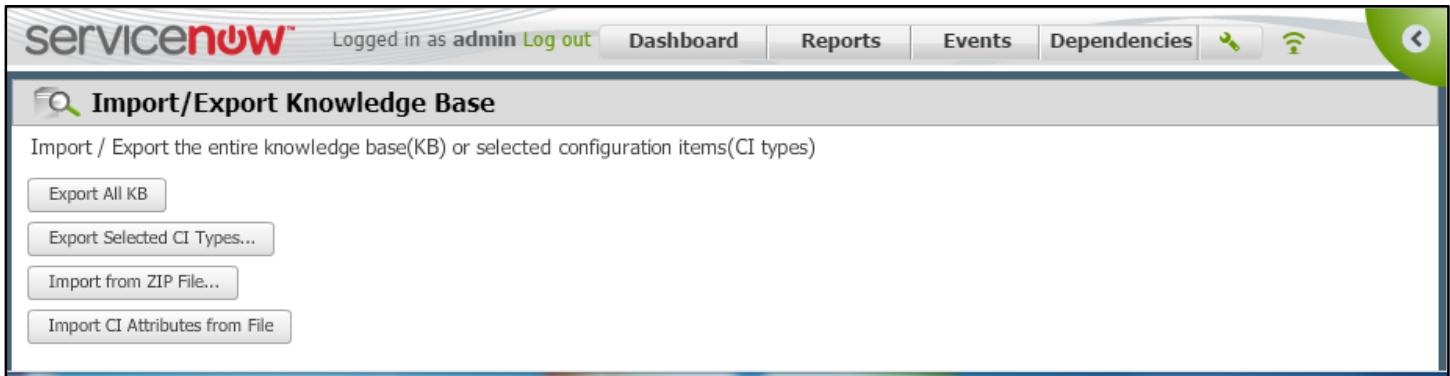
## Import / Export

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.

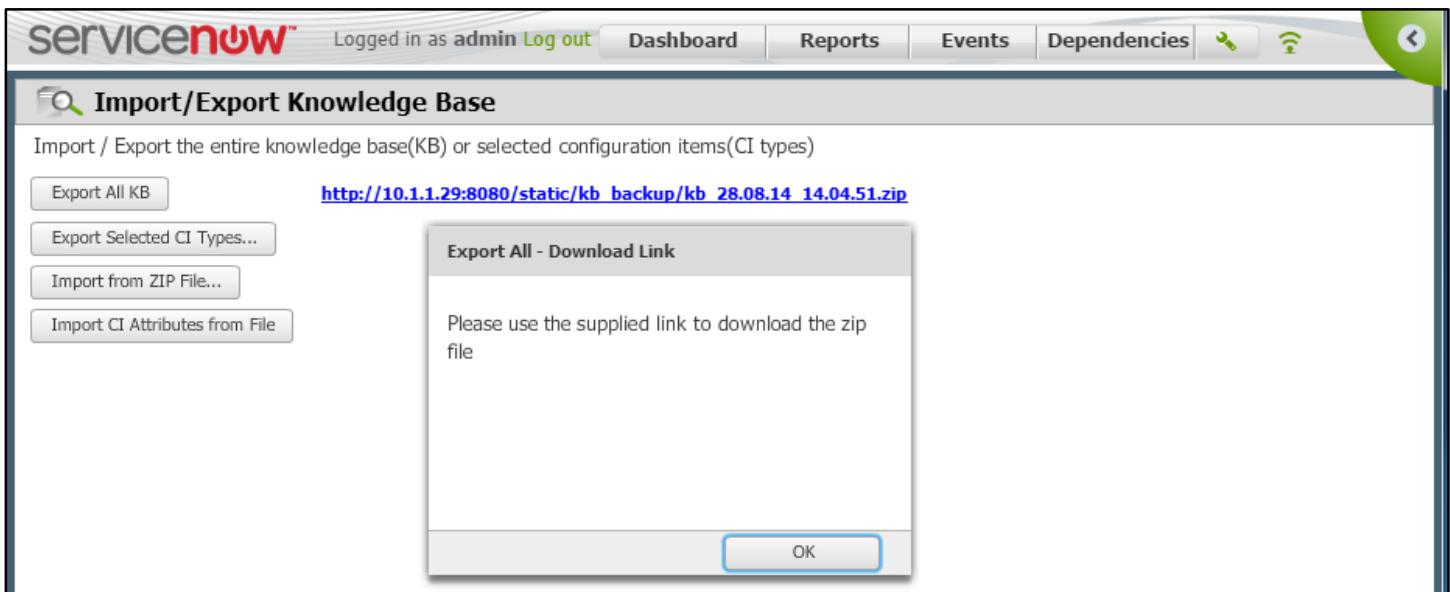
[Figure 81: Import / Export Knowledge Base window](#)



### 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.

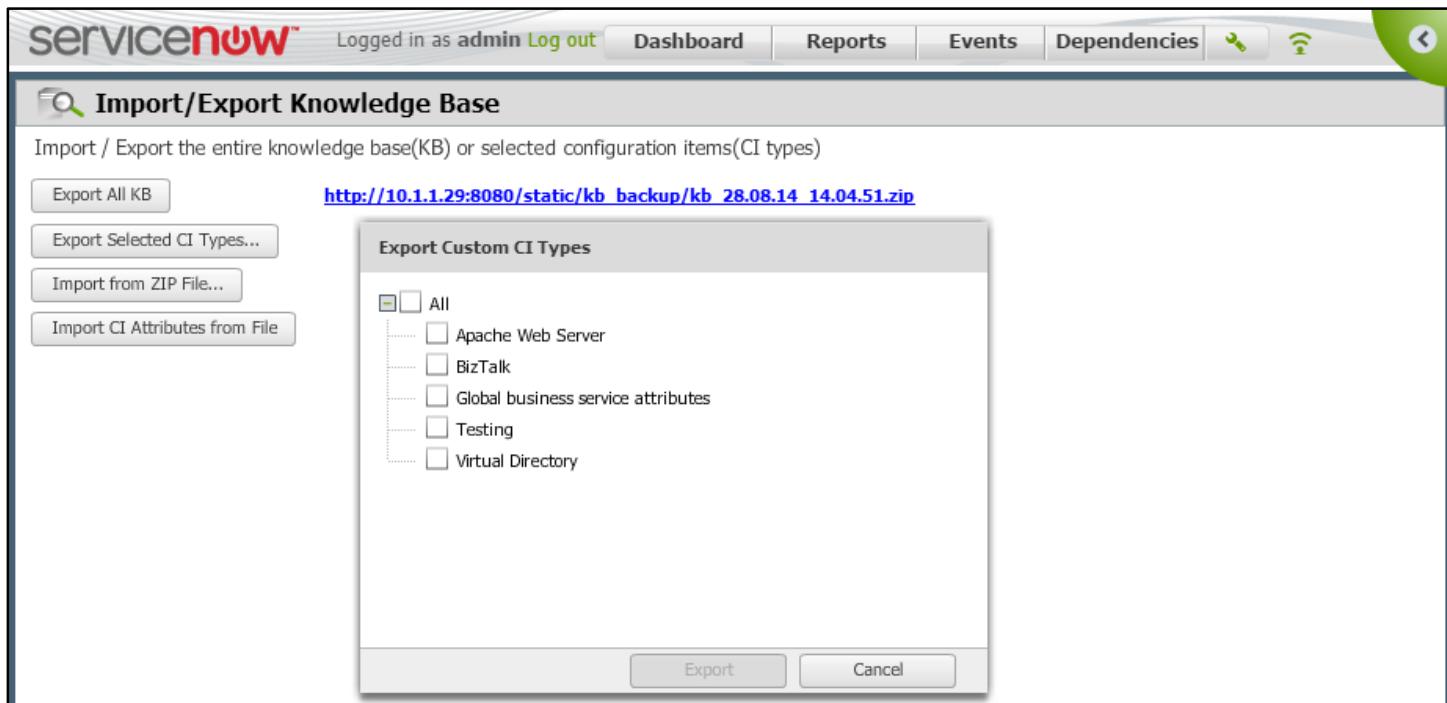
[Figure 82: Export All Download Link message box](#)



## 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

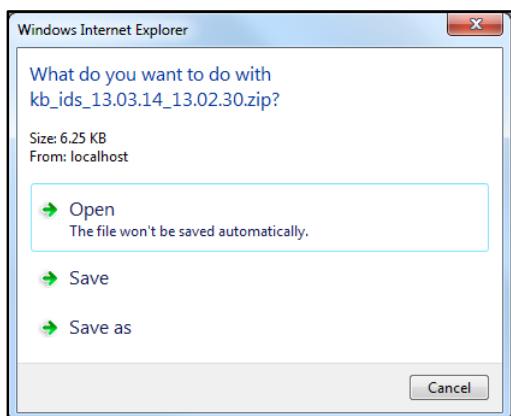


Select the checkboxes of the CI Types you want to export and click **Export**.

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.

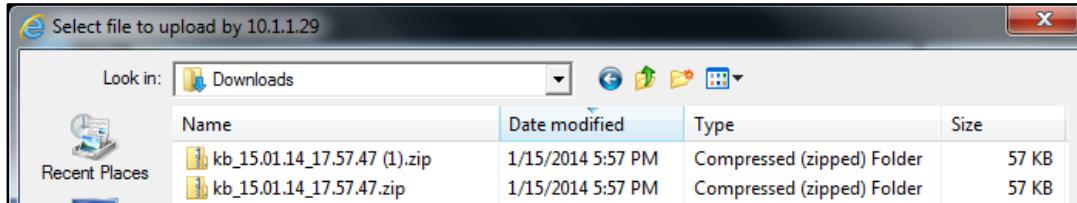
Figure 84: Open, Save, Save as dialog box



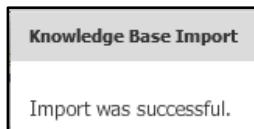
## To import a previously exported file

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.

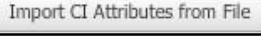
This feature's output includes error messages if the file contains an invalid format or if any line could not be processed for any reason. However, failure to process a line will not abort the update process. The output includes statistics on the number of CIs that were updated and the number of update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

## Chapter 5: Settings

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 Import Output**.

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	1 ▲	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 Files\Java\jdk1.6.0_25\bin\my.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 (milliseconds)		40000
Mail		
Confirm password		***
From		ariel@riel-gordon.com
Password		***
Protocol (smtp or smtps)		smtps
SMTP server		mail.riel-gordon.com
Smtp port		587
User name		riel
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)	<u>10000</u>
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)	<u>30</u>

Parameter	Value
SNMP	
SNMP port	<u>161</u>
SNMP retries	1
SNMP timeout (milliseconds)	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 (milliseconds)	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	

<input checked="" type="checkbox"/> System settings	
Enforce HTTPS protocol. Reload required.	false
Extended call timeout (seconds). Reload required.	600
Invalid serial number REGEX	
Return to dashboard for users. (e.g.: admin, usr_name1, user_name2,....)	
Standard call timeout (seconds). Reload required.	120
Time format (American or European)	American
<input checked="" type="checkbox"/> Traffic based discovery	
Initial netstat frequency (min)	5
Initial netstat samples (Windows, Linux)	12
Initial netstat time between samples in sec (Winodws, Linux)	5
Max. number of connections per CI	1000
Max. number of traffic based connections per CI	30
Netstat discovery excluded CI types	<a href="#">Click to edit</a>
Netstat sniffer discovery	true
Netstat/Sniffer connections purging time (days)	20
Netstat/sniffer connections purging enabled	true
Number of times between initial mode and ongoing mode	10
Ongoing netstat frequency (min)	300
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
<input checked="" type="checkbox"/> WMI	
WMI timeout (milliseconds)	30000

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

**Table 4: Global Parameters**

Parameter Type	Parameter	Description, Comment or Typical Value
<b>3<sup>rd</sup> Party Connectors</b>		
Is Nagios local (true/false)		NetSaint > Nagios Ain't Gonna Insist On Sainthood acronym
Nagios IP address		
<b>Active Directory authentication</b>		
Default role for every user who does not have any assigned role		Click  > Roles to see 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
<b>Alerts</b>		
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
<b>Encryption</b>		
Defines the encryption method: 1 = hard coded, 2 = KeyStore, 3 = file	1	
File location for option 2 or 3	C:\Program Files\Java\jdk1.6.0_25\bin\my.keystore	
Passphrase for option 2		
<b>File tracking</b>		
Max size for each tracked file (KB)	2048	
Max total size of tracked files (MB) on CI.	30	
<b>LDAP</b>		
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
<b>Mail</b>		
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
<b>Middleware</b>		
Define Middleware IP addresses mapping		
<b>Monitoring</b>		
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	
<b>Password Requirements</b>			
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)			
<b>Rediscovery</b>			
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
<b>Reports</b>		
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		
<b>SLA</b>		
SLA compliance default period (days)		Default interval for determining SLA compliance. Value must be more than zero. Typical: 30
<b>SNMP</b>		
SNMP port		
SNMP retries	1	
SNMP timeout (milliseconds)	4000	
<b>SNMP Traps</b>		
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		
<b>SSH</b>		
Privileged command		For example, <b>sudo</b> (super-user <b>do</b> 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 <a href="https://www.mkssoftware.com/docs/man1/stty.1.asp">https://www.mkssoftware.com/docs/man1/stty.1.asp</a> For UNIX , see <a href="http://unixhelp.ed.ac.uk/CGI/man-cgi?stty">http://unixhelp.ed.ac.uk/CGI/man-cgi?stty</a>

Parameter Type	Parameter	Description, Comment or Typical Value
<b>System settings</b>		
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
<b>Traffic based discovery</b>		
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 <b>Initial netstat frequency &amp; samples</b> . Afterwards, the mode is set to <b>ongoing</b> and discovery is based on <b>Ongoing netstat frequency &amp; samples</b> .
Ongoing netstat frequency (min)		300

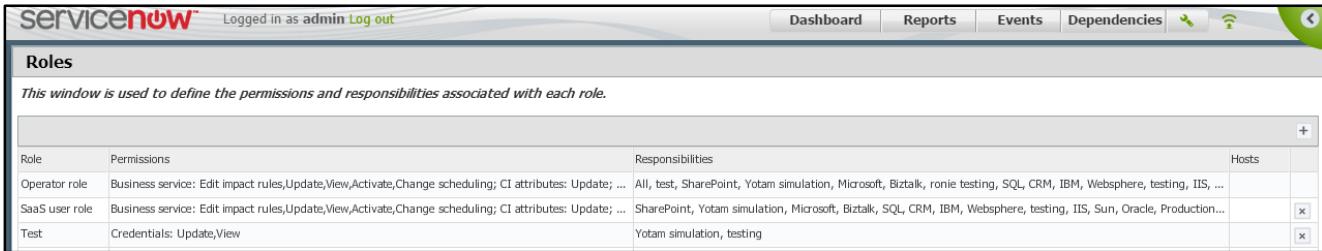
Parameter Type	Parameter	Description, Comment or Typical Value
Ongoing netstat samples (Windows, Linux)	12	
Ongoing netstat time between samples in sec (Windows, Linux)	5	
Process blacklist (regular expression)	system32\\ .+.*(?<!w3wp)\\.exe wininit.exe winlogon.exe indicates outgoing connections from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

## Active Directory feature (LDAP)

To use the LDAP Active Directory feature:

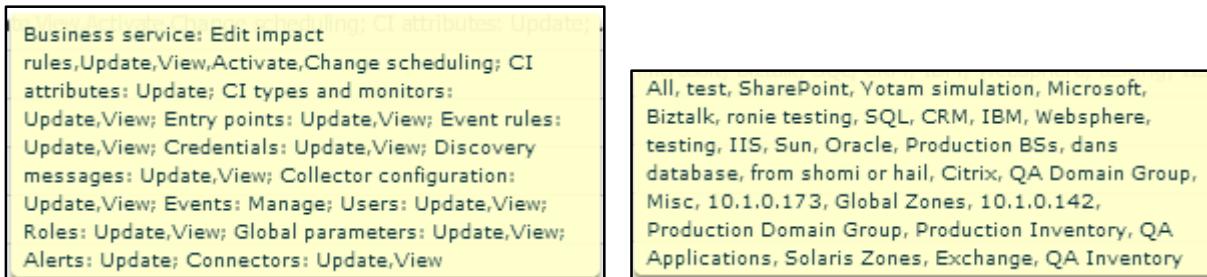
1. Expand the Active directory authentication node in the Global Parameters window and set **Is Active Directory authentication enabled** to true.
2. Click .
3. Select **Settings → Roles** to display the **Roles** window.

Figure 87: Roles window



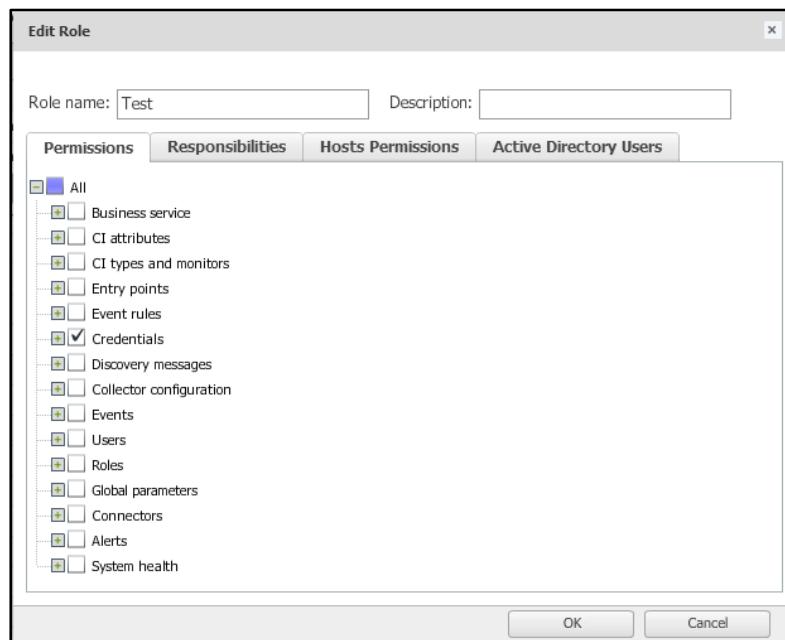
Roles		This window is used to define the permissions and responsibilities associated with each role.	
Role	Permissions	Responsibilities	Hosts
Operator role	Business service: Edit Impact rules, Update, View, Activate, Change scheduling; CI attributes: Update; ...	All, test, SharePoint, Yotam simulation, Microsoft, Biztalk, ronie testing, SQL, CRM, IBM, Websphere, testing, IIS, ...	 
SaaS user role	Business service: Edit Impact rules, Update, View, Activate, Change scheduling; CI attributes: Update; ...	SharePoint, Yotam simulation, Microsoft, Biztalk, SQL, CRM, IBM, Websphere, testing, IIS, Sun, Oracle, Production...	 
Test	Credentials: Update, View	Yotam simulation, testing	 

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



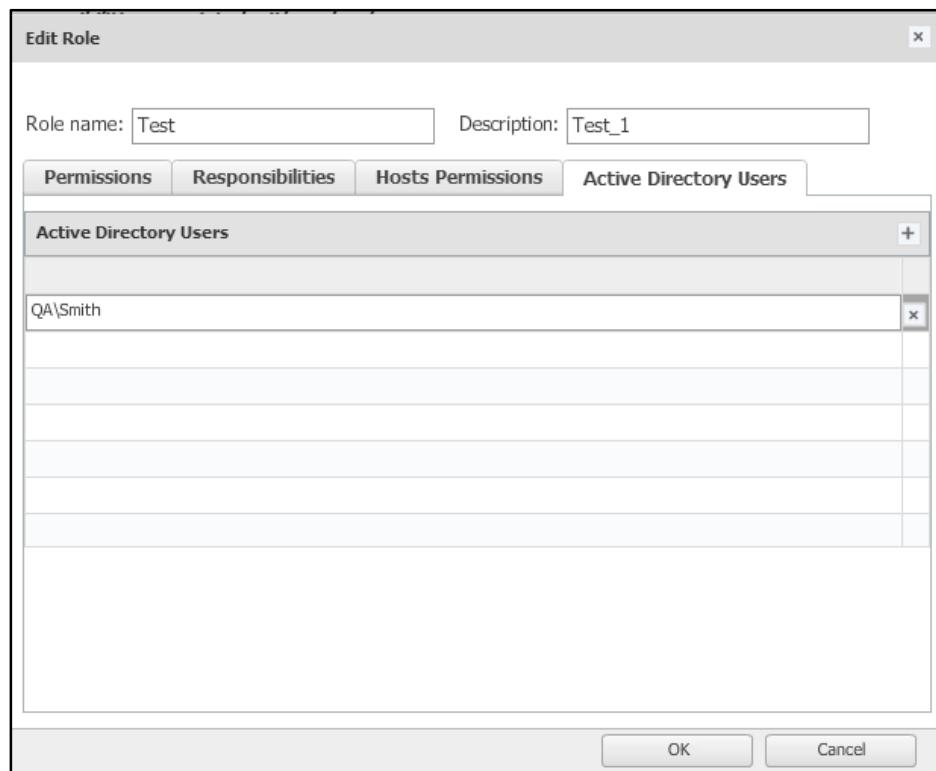
5. Double-click the required role (or first use the + button to add a new role and then double-click it). The **Edit Role** dialog box is displayed.

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**. {0.}

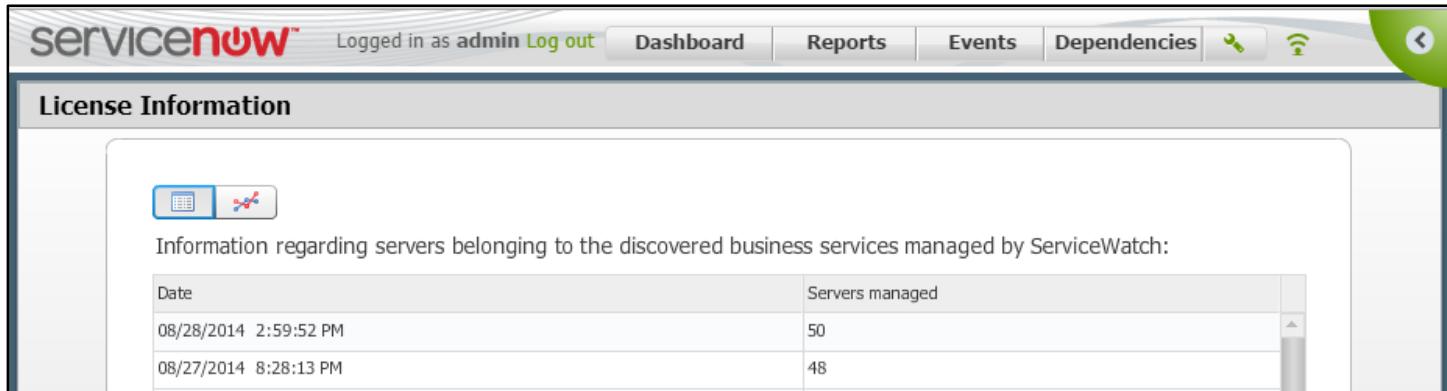
**Figure 90: Role window after adding the DBA role**

Roles			
<i>This window is used to define the permissions and responsibilities associated with each role.</i>			
Role	Permissions	Responsibilities	Hosts
Operator...	Business service: Edit impact rules,Update,View,Act...	All, test, SharePoint, Yotam simulation, Microsoft, Biztalk, ronie testing, SQL, CRM, IBM, Websph...	
SaaS us...	Business service: Edit impact rules,Update,View,Act...	SharePoint, Yotam simulation, Microsoft, Biztalk, SQL, CRM, IBM, Websphere, testing, IIS, Sun, O...	
Test	Credentials: Update,View	Yotam simulation, testing	
DBA	Business service: Edit impact rules,Update,Change ...	All, test, Production BSs, CRM, Solaris Zones, Global Zones, 10.1.0.173, QA Applications, Misc, QA ...	
		<b>Business service:</b> Edit impact rules,Update,Change generic discovery,View,Change scheduling; CI attributes: Update; CI types and monitors: Update,View; Entry points: Update,View; Event rules: Update,View; Credentials: Update,View; Discovery messages: Update,View; Collector configuration: Update,View; Events: Manager; Users: Update,View; Roles: Update,View; Global parameters: Update,View; Connectors: Update,View; Alerts: Update; System health: Update,View	

## License Information

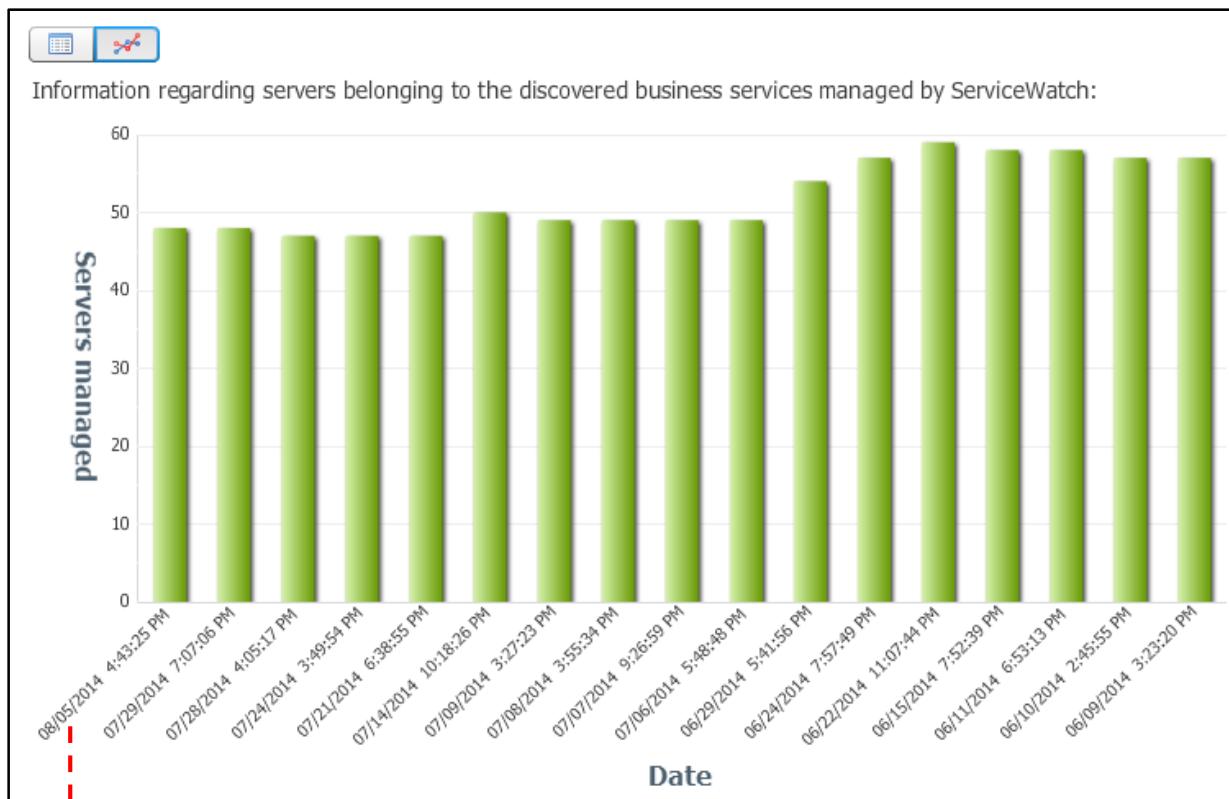
Click the **License Information** link in the **Settings** menu ([Figure 64](#)) to display the **License information** window. This window indicates the number of hosts that were part of the business services on the dates they were discovered. Click the left half of the  icon to display this data as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

This screenshot shows the ServiceNow Roles window. The header bar includes the service logo, a 'Logged in as admin Log out' link, and navigation tabs for Dashboard, Reports, Events, and Dependencies. Below the header is a sub-header 'Roles' with a descriptive note: 'This window is used to define the permissions and responsibilities associated with each role.' The main content is a table with four columns: Role, Permissions, Responsibilities, and Hosts. A tooltip is displayed over the 'Permissions' field for the 'Test' row, showing a detailed list of permissions: Business service: Edit impact rules, Update, View, Activate, Change scheduling; CI attributes: Update; CI types and monitors: Update, View; Entry points: Update, View; Event rules: Update, View; Credentials: Update, View; Discovery messages: Update, View; Collector configuration: Update, View; Events: Manager; Users: Update, View; Roles: Update, View; Global parameters: Update, View; Alerts: Update; Connectors: Update, View.

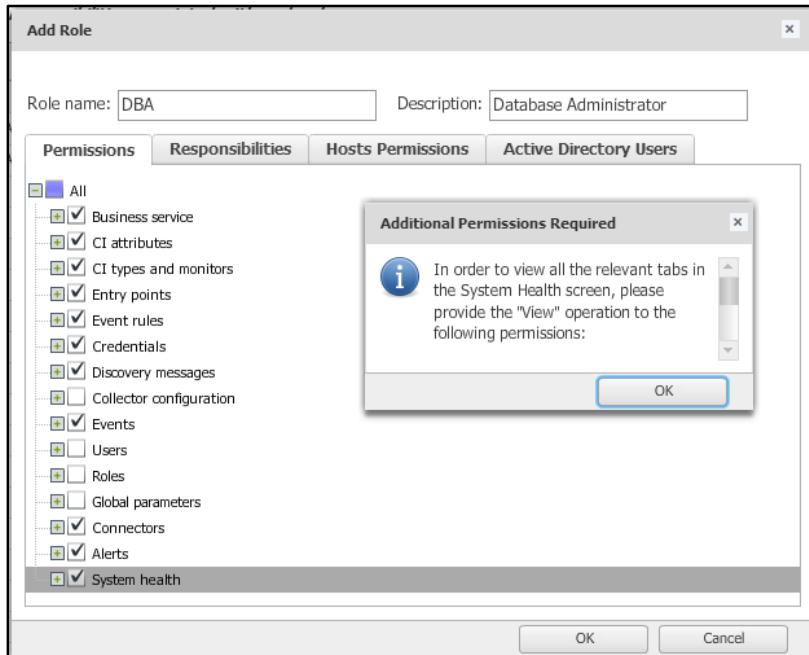
Role	Permissions	Responsibilities	Hosts
Operator ...	Business service: Edit impact rules,Update,View,Activate,Change sched...	All, test, SharePoint, Yotam simulation, Microsoft, Biztalk, ronie testing, SQL, CR...	
SaaS user...	Business service: Edit impact rules,Update,View,Activate,Change sched...	SharePoint, Yotam simulation, Microsoft, Biztalk, SQL, CRM, IBM, Websphere, tes...	x
Test	Credentials: Update,View	Business service: Edit impact rules,Update,View,Activate,Change scheduling; CI attributes: Update; CI types and monitors: Update, View; Entry points: Update, View; Event rules: Update, View; Credentials: Update, View; Discovery messages: Update, View; Collector configuration: Update, View; Events: Manager; Users: Update, View; Roles: Update, View; Global parameters: Update, View; Alerts: Update; Connectors: Update, View	x

This screenshot shows the ServiceNow Roles window, identical to the one above but with a different tooltip. The tooltip for the 'Test' role now displays a longer list of permissions, including additional items like SharePoint, Yotam simulation, Microsoft, Biztalk, SQL, CRM, IBM, Websphere, testing, IIS, Sun, Oracle, Production BSs, dans database, Citrix, QA Domain Group, Misc, 10.1.0.173, Global Zones, 10.1.0.142, Production Domain Group, Production Inventory, QA Applications, Solaris Zones, Exchange, QA Inventory.

Role	Permissions	Responsibilities	Hosts
Operator ...	Business service: Edit impact rules,Update,View,Activate,Change sched...	All, test, SharePoint, Yotam simulation, Microsoft, Biztalk, ronie testing, SQL, CR...	
SaaS user...	Business service: Edit impact rules,Update,View,Activate,Change sched...	SharePoint, Yotam simulation, Microsoft, Biztalk, SQL, CRM, IBM, Websphere, tes...	x
Test	Credentials: Update,View	Yotam simulation, testing, SharePoint, Yotam simulation, Microsoft, Biztalk, SQL, CRM, IBM, Websphere, testing, IIS, Sun, Oracle, Production BSs, dans database, Citrix, QA Domain Group, Misc, 10.1.0.173, Global Zones, 10.1.0.142, Production Domain Group, Production Inventory, QA Applications, Solaris Zones, Exchange, QA Inventory	x

2. Click the icon in the blank header to add a new **Role**. Double-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



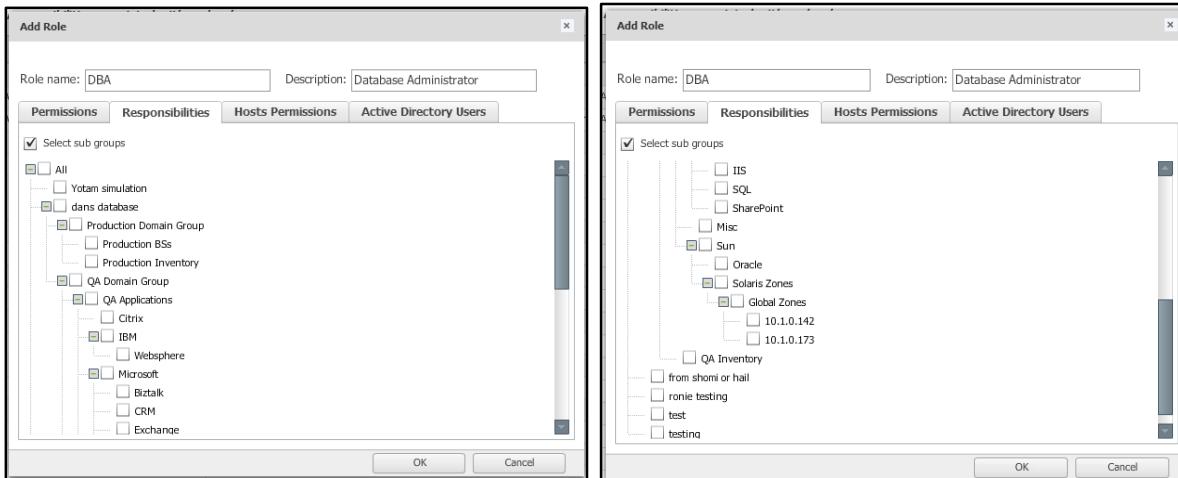
3. If the **Additional Permissions Required** message box is displayed, click its **OK** button after reading it.

#### 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.

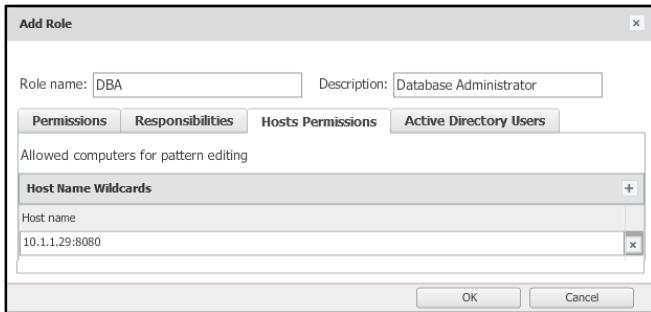
4. Click the **Responsibilities** tab to display a tree that lists business groups. You can expand or collapse the tree. Select the checkbox of the business services or business groups that the role can impact. Select the **All** checkbox to allow this role to apply to every business service.

Figure 95: Add Role window with Responsibilities panel

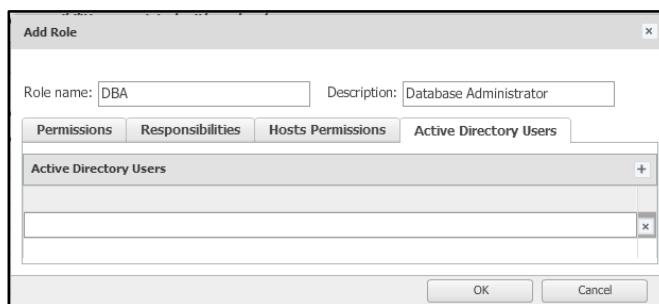


5. To grant permission to define discovery pattern editing on selected hosts, click the **Hosts Permissions** tab. The **Host Permissions** panel is displayed.

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 to save the specified data. Click 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](#)

The screenshot shows the 'Users' window in ServiceNow. At the top, there's a navigation bar with 'Logged in as admin Log out', 'Dashboard', 'Reports', 'Events', 'Dependencies', and some icons. Below the header, a sub-header reads 'Use this screen to define each user and assign the roles he can perform.' A table lists eight users:

User Name	Roles	Account Status	Last successful login	Last unsuccessful login
admin	Administration role	Account is active	08/28/2014 2:03:23 PM	04/27/2014 5:25:39 PM
dba1		Account is active		
demo	Test	Account is active		
operator	Operator role	Account is active		
ronie	Test	Account is disabled	08/19/2014 10:28:43 AM	
saas	SAAS_USER_ROLE	Account is active		
sss	Administration role	Account is active	05/22/2014 4:54:06 PM	
x	Operator role, SAAS_USER_ROLE	Account is active		

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](#)

The 'Add User' dialog box contains the following fields:

- User name:
- Email:
- Description:
- Password:
- Confirm password:

Checkboxes at the bottom left include:
 

- Account is disabled
- Account is locked
- User must change password at next logon

A yellow tooltip above the checkboxes specifies allowed characters: "Allowed in the password: a-z A-Z 0-9 ! @ # \$ % ^ & \* \_ - + =".

The dialog also features two lists for roles:
 

- Available roles:** Administration role, Operator role, SAAS\_USER\_ROLE, Test.
- Assigned roles:** (empty)

 With buttons to move roles between the lists: >> (from Available to Assigned) and << (from Assigned to Available).

At the bottom right are 'OK' and 'Cancel' buttons.

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 OK

To exit the dialog box without saving any data, click Cancel

# 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

The screenshot shows the ServiceNow interface with the title bar "servicenow" and "Logged in as admin Log out". Below the title bar, there are navigation links: Dashboard, Reports, Events, Dependencies, and a search icon. The main content area has a header "Alerts" with the sub-instruction: "This window enables you to specify the triggers for notifications that should be sent when specified changes occur in a business service." A table titled "Alert Rules" is displayed, containing one row with the following details:

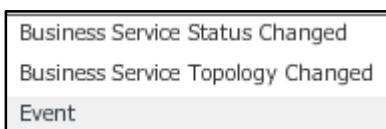
Alert Rules
<pre>Execute the command "nblevent http://10.1.1.124:8080 emsSystem="\${ems}" messageKey="\${msg_key}" resolutionState=\${resolution_state} severity=\${severity} hostAddr... Send mail to ronie.hecker@servicenow.com when received event with severities Information,Minor,Major,Warning or Critical</pre>

A tooltip is shown over the second item in the list, containing the same command text. The tooltip is styled with a yellow background and black text.

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.

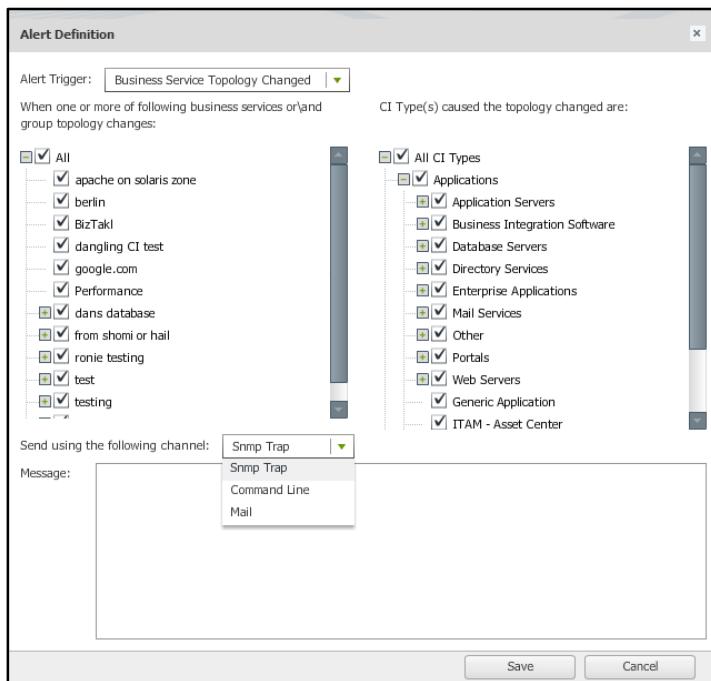
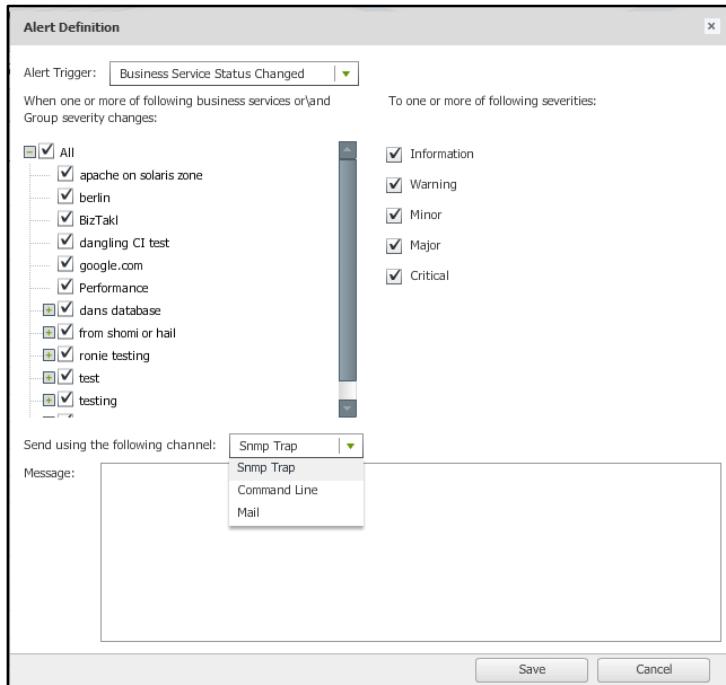
The **Alert Definition** dialog is displayed. It has 3 variations determined by the **Alert Trigger** value:

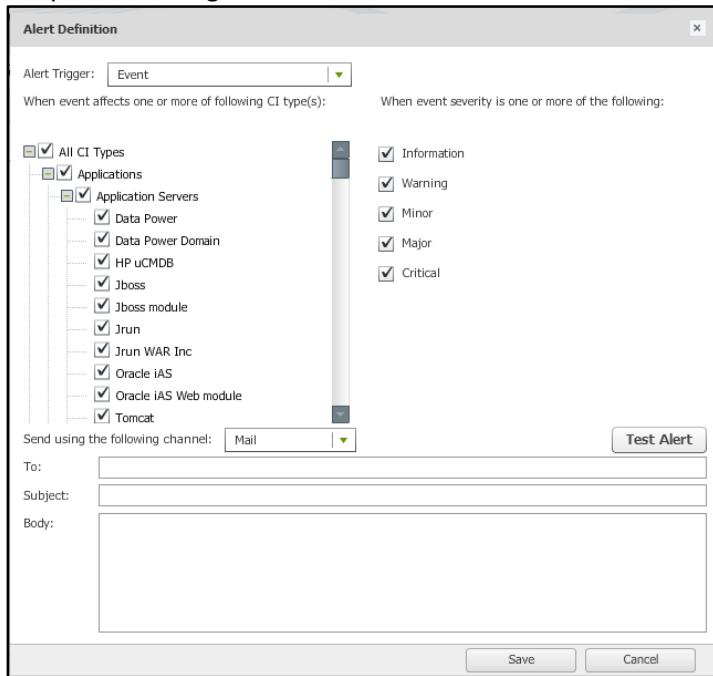


Click the **Alert Trigger** green down-arrow to select the type of trigger. One of these three dialog boxes is displayed.

## Chapter 5: Settings

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

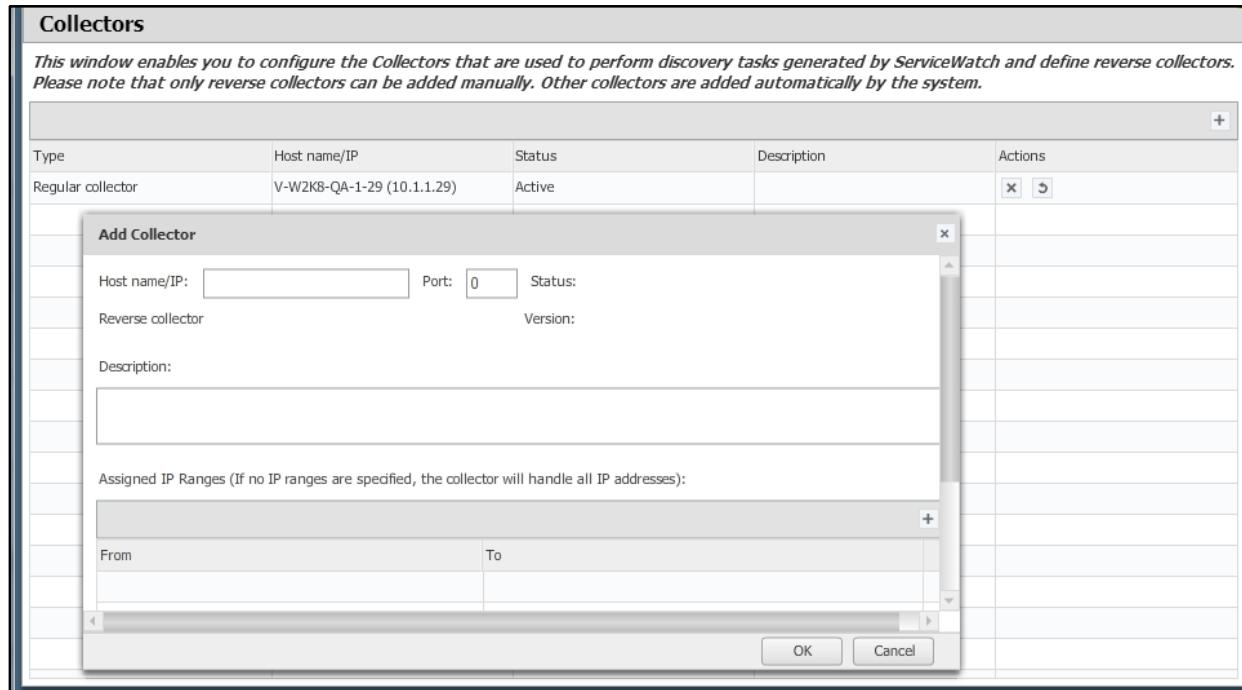
The ServiceWatch architecture consists of one Server plus one or more Collectors.

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 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

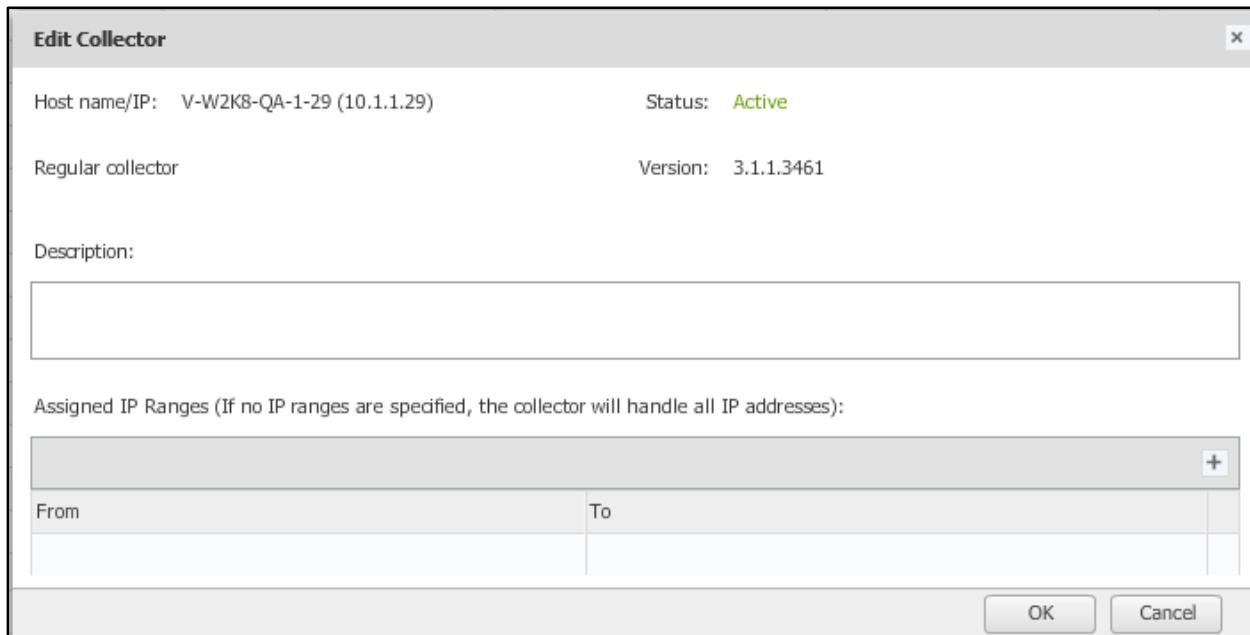
To restart a listed collector, click the icon in the **Actions** column on the row of that collector.

## 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 or 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 credentials you supply are encrypted and totally secure against unauthorized use.
- 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](#)

The screenshot shows the ServiceNow interface with the title bar "servicenow" and "Logged in as admin Log out". Below the title bar, there are navigation links for "Dashboard", "Reports", "Events", and "Dependencies". On the far right, there are icons for search, refresh, and help.

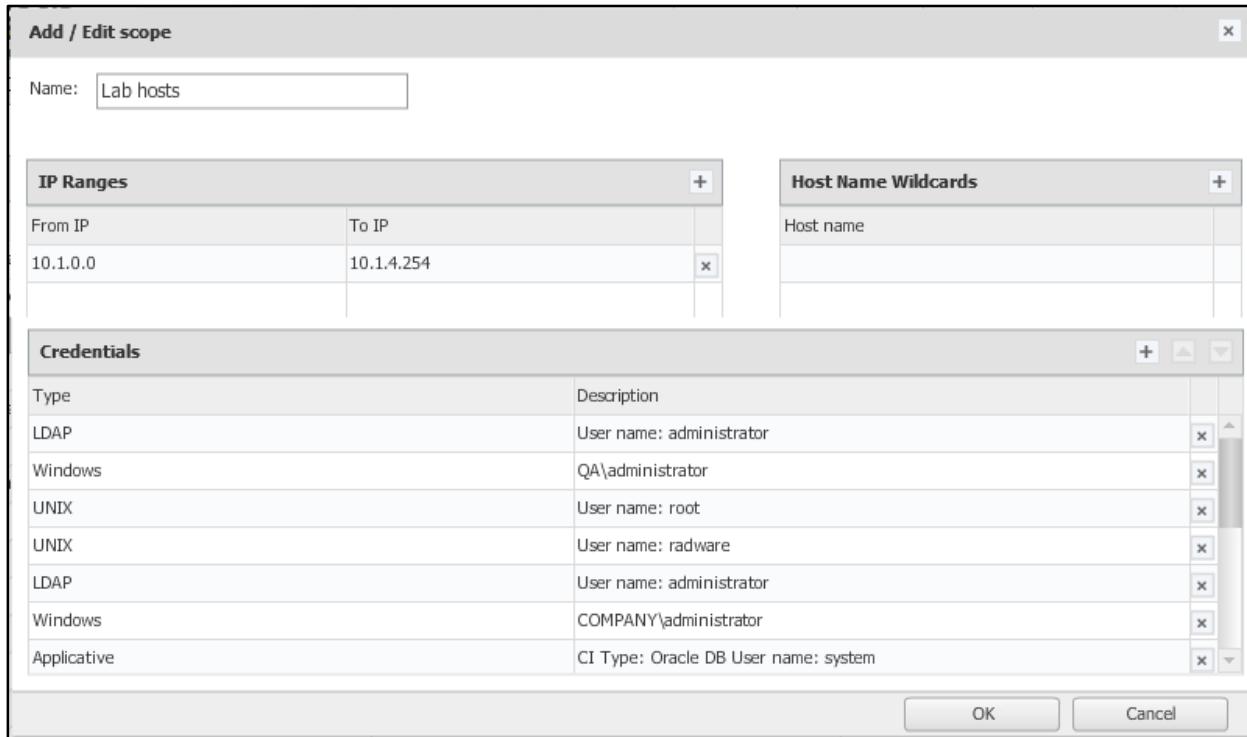
The main content area is titled "Credentials". A sub-instruction below the title reads: "This screen enables you to define the credentials that ServiceWatch needs to communicate with remote hosts during the discovery process."

A table lists the defined credentials:

Name	IP Address Ranges	Host Name Wildcards	Action
Factory Applicative Credentials	0.0.0.0 - 255.255.255.255	*	<input type="button" value="X"/>
Production Credentials	172.16.1.1 - 172.16.1.254		<input type="button" value="X"/>
Lab hosts	10.1.0.0 - 10.1.4.254		<input type="button" value="X"/>
sun	192.168.200.50 - 192.168.200.50		<input type="button" value="X"/>
Neebula test scope	1.0.0.0 - 255.255.255.255	*	<input type="button" value="X"/>
Avi Test	10.1.4.20 - 10.1.4.20		<input type="button" value="X"/>
Leonid credentials	10.1.1.132 - 10.1.1.132		<input type="button" value="X"/>
live demo	0.0.0.0 - 255.255.255.255		<input type="button" value="X"/>

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
<p><b>Add / Edit Credentials</b></p> <p>Type: <b>UNIX</b></p> <p>Login type: <input checked="" type="radio"/> sudo <input type="radio"/> super user <input type="radio"/> local super user</p> <p><input type="checkbox"/> CI Type: _____</p> <p>User name: _____</p> <p>You must fill at one of the following fields: Password, SSH Private key with Passphrase or Super user password.</p> <p>Password: _____</p> <p>Confirm password: _____</p> <p>SSH private key: _____</p> <p>Passphrase: _____</p> <p>Confirm passphrase: _____</p> <p>IP/Host: _____ <input type="button" value="Test credentials"/></p> <p style="text-align: center;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>	<p><b>Add / Edit Credentials</b></p> <p>Type: <b>SNMP</b></p> <p>SNMP version: <input type="radio"/> SNMP v1/2c <input checked="" type="radio"/> SNMP v3</p> <p>User name: _____</p> <p>Security level: <b>AuthPriv</b></p> <p>Authentication protocol: <b>MD5</b></p> <p>Authentication password: _____</p> <p>Privacy protocol: <b>DES</b></p> <p>Privacy password: _____</p> <p>Context engine ID: _____</p> <p>Context name: _____</p> <p>IP/Host: _____ <input type="button" value="Test credentials"/></p> <p style="text-align: center;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>
Applicative	Windows
<p><b>Add / Edit credentials</b></p> <p>Type: <b>Applicative</b></p> <p>CI Type: _____</p> <p>User Name: _____</p> <p>Password: _____</p> <p>Confirm Password: _____</p> <p style="text-align: center;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>	<p><b>Add / Edit credentials</b></p> <p>Type: <b>Windows</b></p> <p><input type="checkbox"/> CI Type: _____</p> <p>Domain: _____</p> <p>User Name: _____</p> <p>Password: _____</p> <p>Confirm Password: _____</p> <p>IP/Host: _____ <input type="button" value="Test credentials"/></p> <p style="text-align: center;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>
LDAP	NetApp
<p><b>Add / Edit credentials</b></p> <p>Type: <b>LDAP</b></p> <p>User Name: _____</p> <p>Password: _____</p> <p>Confirm Password: _____</p> <p>IP/Host: _____ <input type="button" value="Test credentials"/></p> <p style="text-align: center;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>	<p><b>Add / Edit credentials</b></p> <p>Type: <b>NetApp</b></p> <p>User Name: _____</p> <p>Password: _____</p> <p>Confirm Password: _____</p> <p>IP/Host: _____ <input type="button" value="Test credentials"/></p> <p style="text-align: center;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>

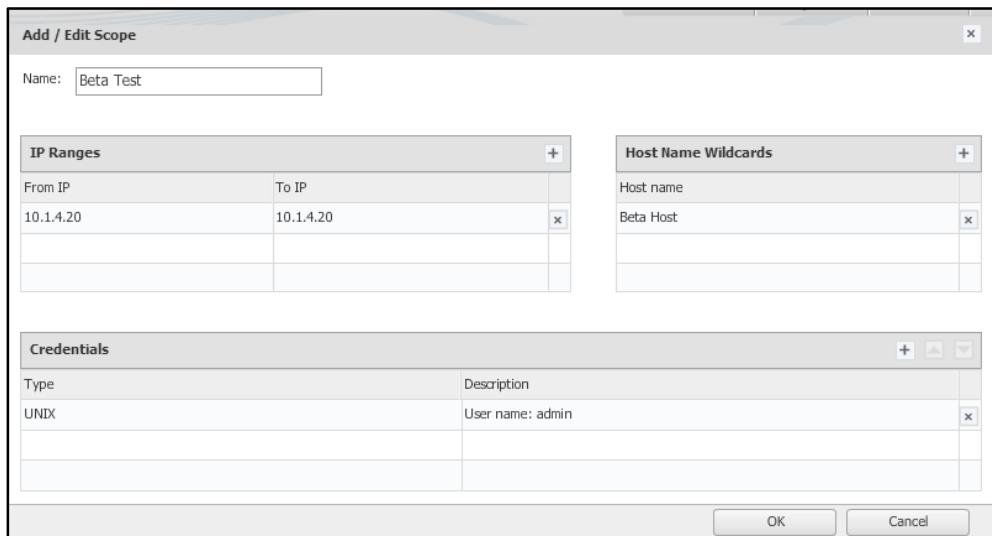
7. Define the credentials. To edit an existing value, click the relevant field and modify the value.
  - a. Select the credential **Type** from the drop-down list. The fields displayed in the dialog box vary based on the credential **Type**.
  - b. Fill in the dialog box fields. If you select **Applicative** 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 in the **Add/Edit credentials** dialog box or click 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 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](#)



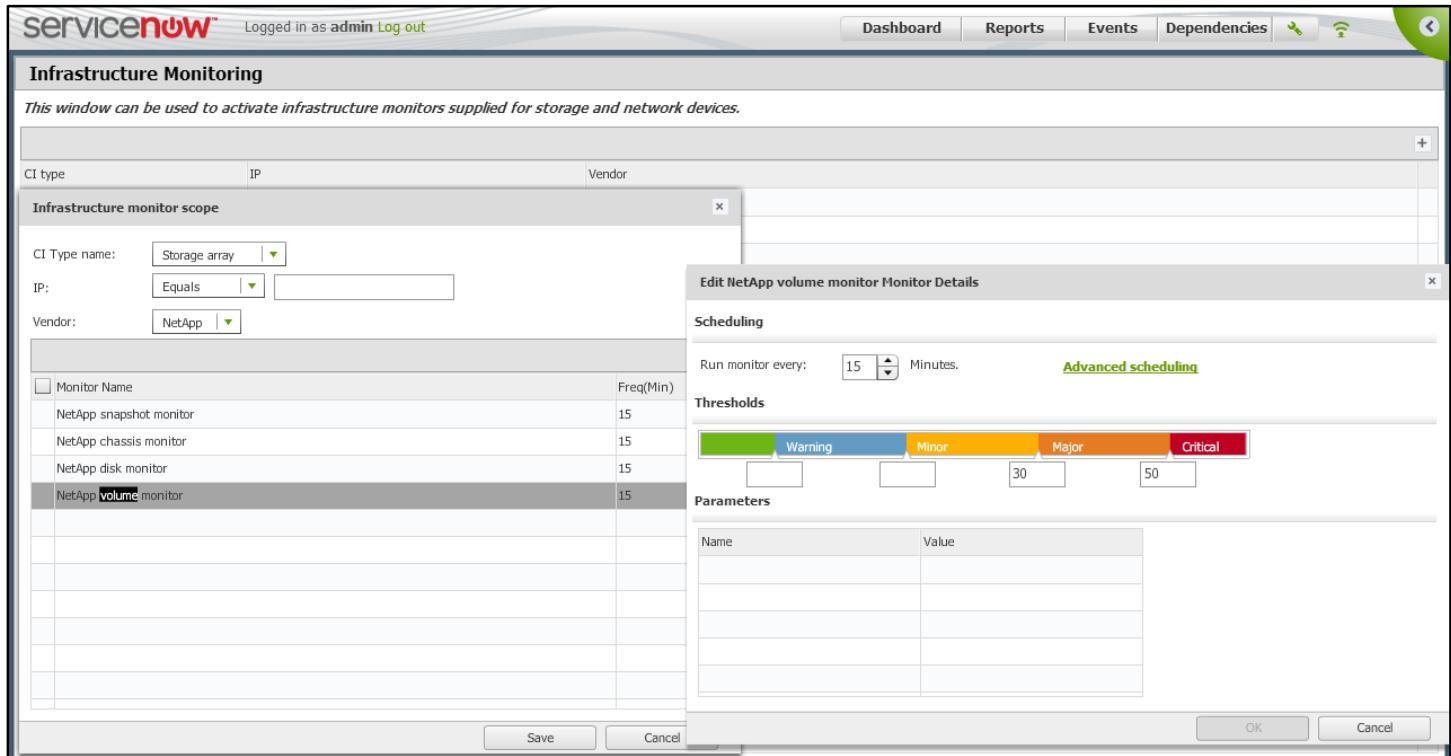
**Figure 107: Credentials window after adding a Credential**

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	*	<input type="button" value="x"/>
Production Credentials	172.16.1.1 - 172.16.1.254		<input type="button" value="x"/>
Lab hosts	10.1.0.0 - 10.1.4.254		<input type="button" value="x"/>
sun	192.168.200.50 - 192.168.200.50		<input type="button" value="x"/>
Neebula test scope	1.0.0.0 - 255.255.255.255	*	<input type="button" value="x"/>
Avi Test	10.1.4.20 - 10.1.4.20		<input type="button" value="x"/>
Leonid credentials	10.1.1.132 - 10.1.1.132		<input type="button" value="x"/>
live demo	0.0.0.0 - 255.255.255.255		<input type="button" value="x"/>
Beta Test	10.1.4.20 - 10.1.4.20	Beta Host	<input type="button" value="x"/>

## 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 or to exit the **Edit <Monitor name> Monitor Details** dialog box.

In the **Infrastructure monitor scope** dialog box, click to exit without saving or 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

The screenshot shows the ServiceNow interface with the 'Monitoring Connectors' page open. A modal dialog box titled 'Add New 3rd Party Connector' is displayed in the center. The dialog contains fields for '3rd Party Component' (set to 'Connector for EMC Symmetrix'), 'Frequency (Mins)' (set to '60'), 'Description' (empty), 'IP/Host name' (highlighted with a red border), 'SymCLI executables path' (highlighted with a red border), and a checked 'Run As Superuser' checkbox. Below the fields are 'Test Connection' and 'Save' buttons. In the background, the main table lists one connector: 'Monitoring Connector' named 'scom2012' with 'User Name' 'qa\administrator'. The top navigation bar includes 'Dashboard', 'Reports', 'Events', and 'Dependencies'.

To add a 3rd party connector, click in the top right corner of the **Monitoring Connectors** table.

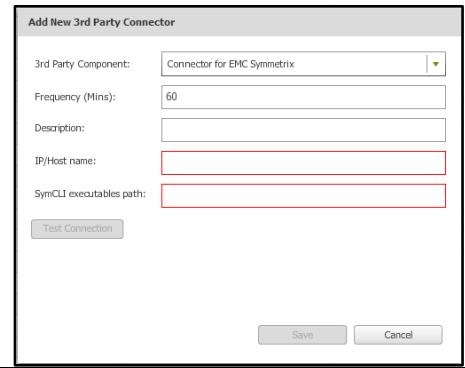
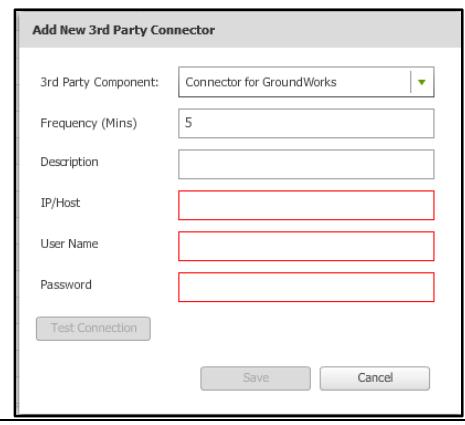
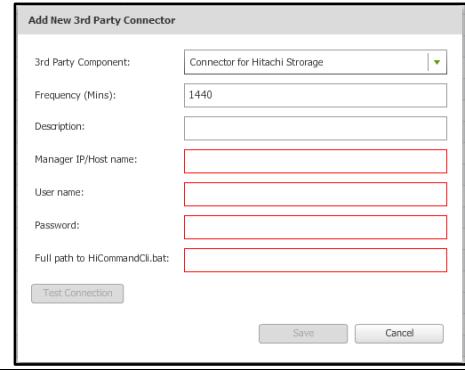
In the **Add New 3rd Party Connector** dialog box, use the down-arrow to select the **3rd Party Component** that is connected. ServiceWatch supports components such as: EMC Symmetrix, GroundWorks, HP EVA, IMAP, Netcool on Unix, Netcool on Windows, POP3, SolarWinds, Splunk, HP OpenView Unix, and Microsoft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

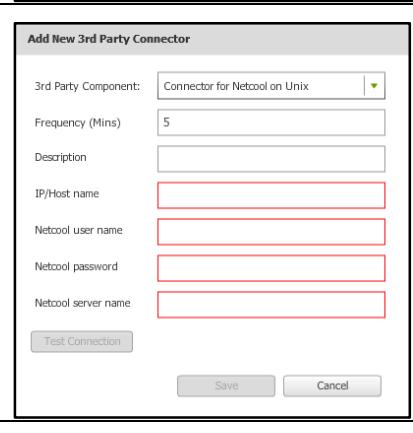
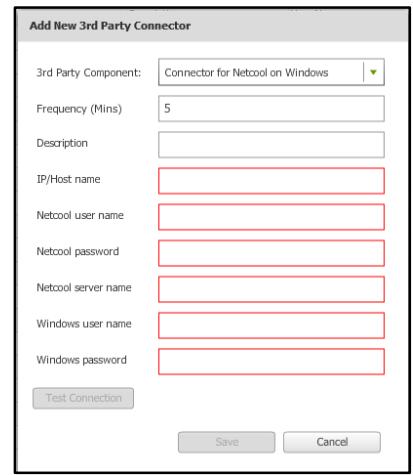
To modify an existing connector, double-click its row in the **Monitoring Connectors** table. The **Update 3<sup>rd</sup> Party Connector** window will be displayed.

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

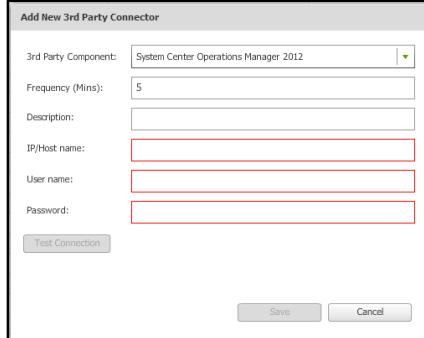
Click . If the test is successful, click . Otherwise, correct the values and test again or click to exit the dialog box without saving the data in it.

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

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

	<p><a href="#">Internet Message Access Protocol (IMAP)</a> allows an <a href="#">e-mail client</a> to access <a href="#">e-mail</a> on a remote <a href="#">mail server</a>. IMAP servers usually listen on port 143. IMAP over <a href="#">SSL</a> (IMAPS) is assigned port 993. IMAP supports <a href="#">on-line</a> and <a href="#">off-line</a> 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 <i>clients</i> support IMAP in addition to <a href="#">Post Office Protocol (POP)</a>.</p>
	<p>IBM Tivoli Netcool 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 <a href="#">link</a>.</p>
	<p>For data about configuring IBM Tivoli Netcool properties and server communications for Windows, use this <a href="#">link</a>.</p>
	<p><b>Post Office Protocol (POP3)</b> is used by local <a href="#">e-mail clients</a> to retrieve <a href="#">e-mail</a> from a remote <a href="#">server</a> over a <a href="#">TCP/IP</a> connection. Almost all e-mail clients and <a href="#">servers</a> support POP3. <a href="#">Webmail</a> service providers such as <a href="#">Google Mail</a>, <a href="#">Microsoft Mail</a> and <a href="#">Yahoo! Mail</a> support IMAP and POP3.</p>

	<p><a href="#">SolarWinds</a> Network Performance Monitor detects, diagnoses and resolves network performance problems and outages.</p>
	<p><a href="#">Splunk Enterprise</a> converts the machine data generated by IT systems and technology infrastructure into information about the status of computer networks and applications running on them.</p>
	<p>For information about integrating HP OpenView operations on UNIX, see this <a href="#">link</a>.</p>
	<p>For information about <a href="#">System Center Operations Manager</a>, see  <a href="http://www.networkworld.com/article/2230377/microsoft-subnet/understanding-how-system-center-operations-manager-works.html">http://www.networkworld.com/article/2230377/microsoft-subnet/understanding-how-system-center-operations-manager-works.html</a></p> <p>For data about System Center Operations Manager 2007, see  <a href="http://technet.microsoft.com/en-us/library/bb310604.aspx">http://technet.microsoft.com/en-us/library/bb310604.aspx</a></p>

	<p>For data about <a href="#">System Center Operations Manager 2012</a>, see  <a href="http://technet.microsoft.com/en-us/library/hh205987.aspx">http://technet.microsoft.com/en-us/library/hh205987.aspx</a></p>
---	---

## 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 **Traffic Based Discovery** 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**

The screenshot shows the ServiceNow Network Discovery window. At the top, there are summary statistics: Total hosts: 262, Subnets: 37, Network devices: 72, Discovery messages on network devices: 261, Routers: 3, and Switches: 5. Below this, there's a section for 'Include/Exclude IP Ranges' with a table where users can specify 'From' and 'To' IP addresses. There's also a 'Save' and 'Cancel' button at the bottom right.

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 button. If you enter an invalid IP or Host, an error is displayed in the Network Discovery panel (see page 69).
6. 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

The screenshot shows the ServiceNow interface with the title bar "service<sup>now</sup>" and "Logged in as admin Log out". Below the title bar, there are navigation links for "Dashboard", "Reports", "Events", and "Dependencies". On the right side of the header, there are icons for search and refresh. The main content area has a title "Virtualization Connectors". Below the title is a table with the following data:

Category	Name	URL	Description	User Name
Virtualization Connector	VMware vCenter	https://172.16.1.45		neebula\vrnd

At the bottom right of the table are two buttons: "Save" and "Cancel".

To add a new 3<sup>rd</sup> 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

The image displays four separate dialog boxes, each titled "Add New 3rd Party Connector".

- AWS Connector:** Set "3rd Party Component" to "Connector for AWS". "Frequency (Mins)" is set to 60. "AWS Access Key" and "AWS Secret Key" fields are highlighted in red.
- EMC ECC Connector:** Set "3rd Party Component" to "Connector for EMC ECC". "Frequency (Mins)" is set to 60. "Description", "IP/Host", "Port", "URL", "User Name", and "Password" fields are highlighted in red. An "isSSL" checkbox is present.
- vCenter Connector:** Set "3rd Party Component" to "Connector for vCenter". "Frequency (Mins)" is set to 1440. "URL", "User Name", and "Password" fields are highlighted in red. A "Test Connection" button is present.
- XEN Connector:** Set "3rd Party Component" to "Connector for XEN". "Frequency (Mins)" is set to 60. "Description", "URL", "User Name", and "Password" fields are highlighted in red. A "Test Connection" button is present.

In all dialog boxes, there are "Save" and "Cancel" buttons at the bottom.

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

- [CONCEPTS](#)
- [BUSINESS GROUPS](#)
- [CREATING TECHNICAL BUSINESS SERVICES](#)
- [ROOT CAUSE ANALYSIS](#)
- [BUSINESS SERVICE, OBJECT OR CONNECTION PROPERTIES](#)
- [VIEWING THE IMPACT TREE OF A BUSINESS SERVICE](#)
- [WORKING WITH EXISTING BUSINESS SERVICES & GROUPS](#)
- [EDITING A BUSINESS SERVICE](#)
- [ADJUSTING THE TOPOLOGY MAP](#)

**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 [132](#).

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 149.

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 132).

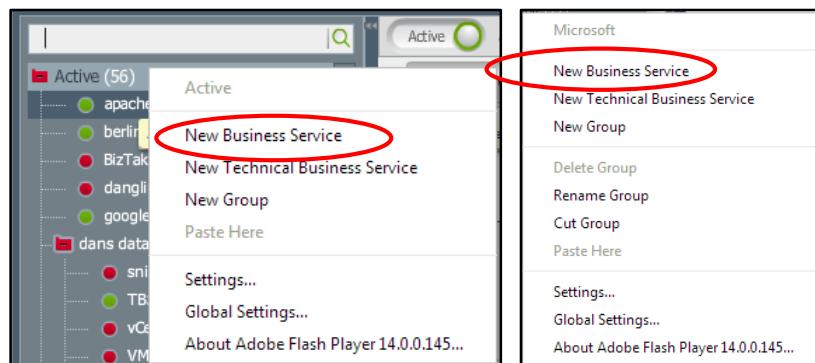
To create a Technical Business Service, see [CREATING TECHNICAL BUSINESS SERVICES](#) on page 149.

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

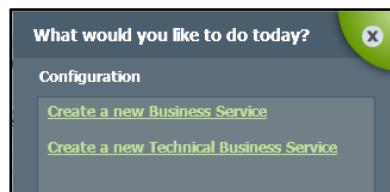
- Adjust the screen display. For details, see [Adjusting the Topology Map](#) on page 161.
- Collapse or expand groups in the topology displays
- Display business services in the Dashboard by selecting the Active root or by clicking the Dashboard button until the Dashboard is displayed.
- Work on a different 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**

The screenshot shows the 'Definition' tab of the Business Service wizard. The 'Business service name' field contains 'Performance'. The 'Related groups' dropdown menu is open, showing 'testing' as the selected item. The 'Business service priority' dropdown menu is open, showing '4' as the selected value. A note below the priority dropdown says: 'Mandatory field: Please provide the URL(s) below, that users use to access the business service'.

- 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**

The screenshot shows the 'Entry Points' pane. It includes a 'Type' dropdown set to 'HTTP(S)', a 'Description' input field, and a large 'URL' input field which is currently empty and highlighted with a red border.

- 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**

The screenshot shows the 'Entry Points' pane with the 'Type' dropdown set to 'MS SQL Server'. Below the dropdown, three additional fields are visible: 'Host', 'DB instance name', and 'Port', each with its own input field.

- d. For each additional entry point, click **Add another entry point** 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

Less details

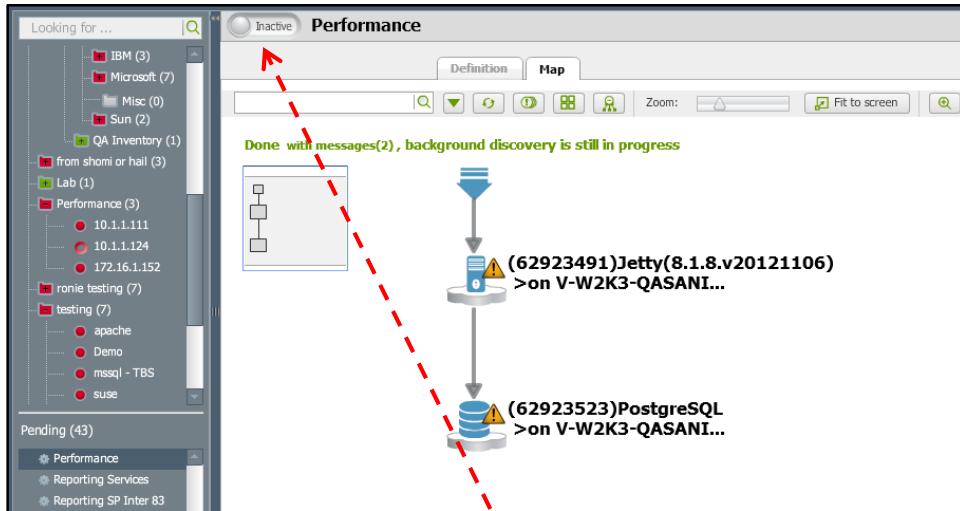
Owner email: [ ] Owner name: [ ]

Owner phone: [ ] Traffic based discovery: True ▾

Save and view Map

- When you finish defining entry points, click **Save and view Topology** 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



- To activate this business service, click **Inactive** in the top left corner. The business service's state indicator will change to **Active** and it will move from the **Pending** panel to the **Active** tree. To disable this business service, click **Active**. The business service's state indicator will change to **Inactive** and it will move from the **Active** tree to the **Pending** panel.

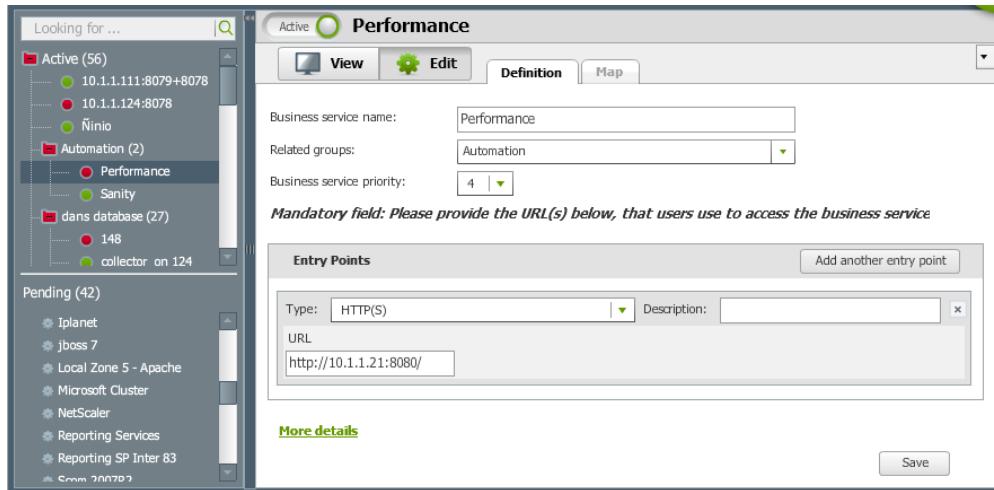
- When the business service is **Active**, the **View/Edit** toggle buttons are displayed. Click **View** to view the topology **Map**.



## Performing Manual Operations

- When the business service is Active, 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**



- If you modify the business service definition *without* changing **Entry points** data, a **Save** button lets you save the changes without invoking the Discovery process. If you do change **Entry points** data, the **Save** 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 139.

### Adjusting the topology map

- 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

- For an explanation of object impact rules and instructions for defining them by status, see [DEFINING OBJECT IMPACTS ON THE BUSINESS SERVICE](#) on page 140. 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.
- 
- Please select the class of rediscovery frequency:
- Rare  
 Normal  
 Frequent
- 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.

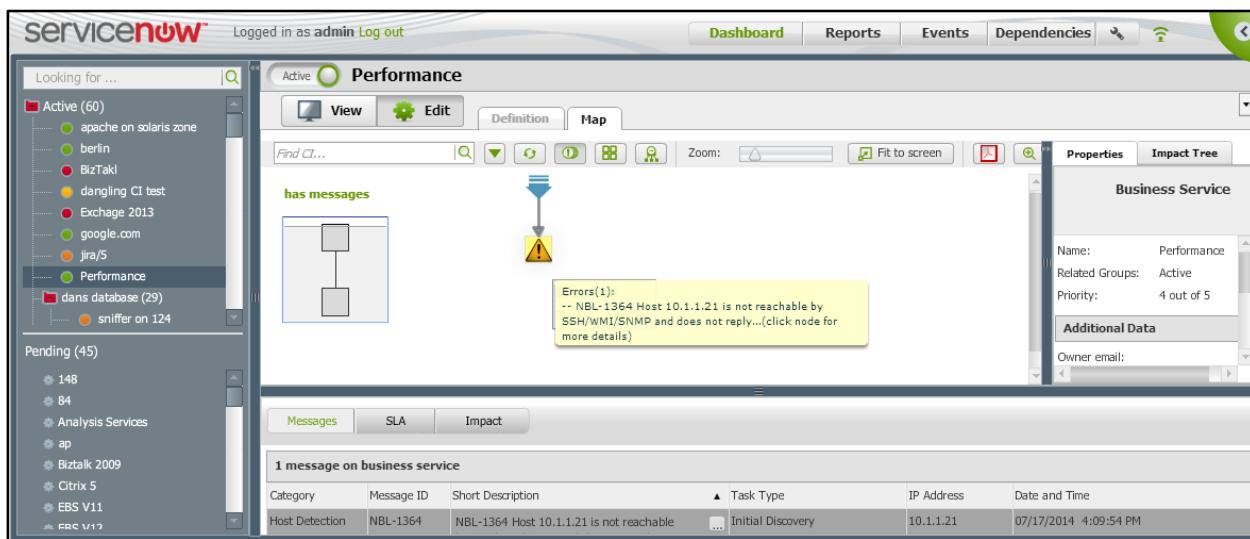
## Adjusting the Business Service Topology

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 .

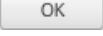
Adjustment options are described in [TABLE 5](#) for Objects and in [TABLE 6](#) for Connection lines.

**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 <b>Entry Point</b> 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 <b>Dependencies</b> 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  . 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: <ul style="list-style-type: none"> <li>✓ Fill in the business service name</li> <li>✓ Select the group name (optional)</li> <li>✓ Select the priority</li> <li>✓ Click .</li> </ul> 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 <b>Unmark as Boundary</b> .
Remove Manual Connection	Removes a connection that was added manually via Add Connection. To remove a discovered connection, use <b>Mark as Boundary</b> .
Resume discovery	Enables discovery to resume from a particular node.
Show network path	Displays the network path and information about it. See <a href="#">Table 8</a> and <a href="#">CHAPTER 10: MONITORING NETWORKS</a> .
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).
- 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:

No impact rule definition for the selected node.

If the selected node is inside a cluster the impact for it is set through its parent cluster.

If a storage array or network path node was selected the impact for it is set through the business service impact definitions.

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.

- 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**

Source	Target	% Influence
Critical	Critical	100
Major	Major	100
Minor	Minor	100
Warning	Warning	100

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

- 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**

Source	Target	% Influence
Critical	Critical	100
Major	Major	100
Minor	Minor	100
Warning	Warning	100

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.

- 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

Source	Target	% Influence
Critical	Critical	100
Major	Major	100
Minor	Minor	100
Warning	Warning	100

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

Source	SSIS Standard Edition on MSSQLSERVER		SSMS-Import-From-Excel	
	Target	% Influence	Target	% Influence
Critical	Critical	100	Critical	100
Major	Major	100	Major	100
Minor	Minor	100	Minor	100
Warning	Warning	100	Warning	100

## 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

Source	Target	Redundancy Target
Critical	Critical	Major
Major	Major	Minor
Minor	Minor	Warning
Warning	Warning	Information

## 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

Source	Target
Critical	Critical
Major	Major
Minor	Minor
Warning	Warning

## 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

Source	Target	Redundancy Target
Critical	Critical	Major
Major	Major	Minor
Minor	Minor	Warning
Warning	Warning	Information

## 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

Source	Target	Redundancy Target
Critical	Critical	Major
Major	Major	Minor
Minor	Minor	Warning
Warning	Warning	Information

## 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

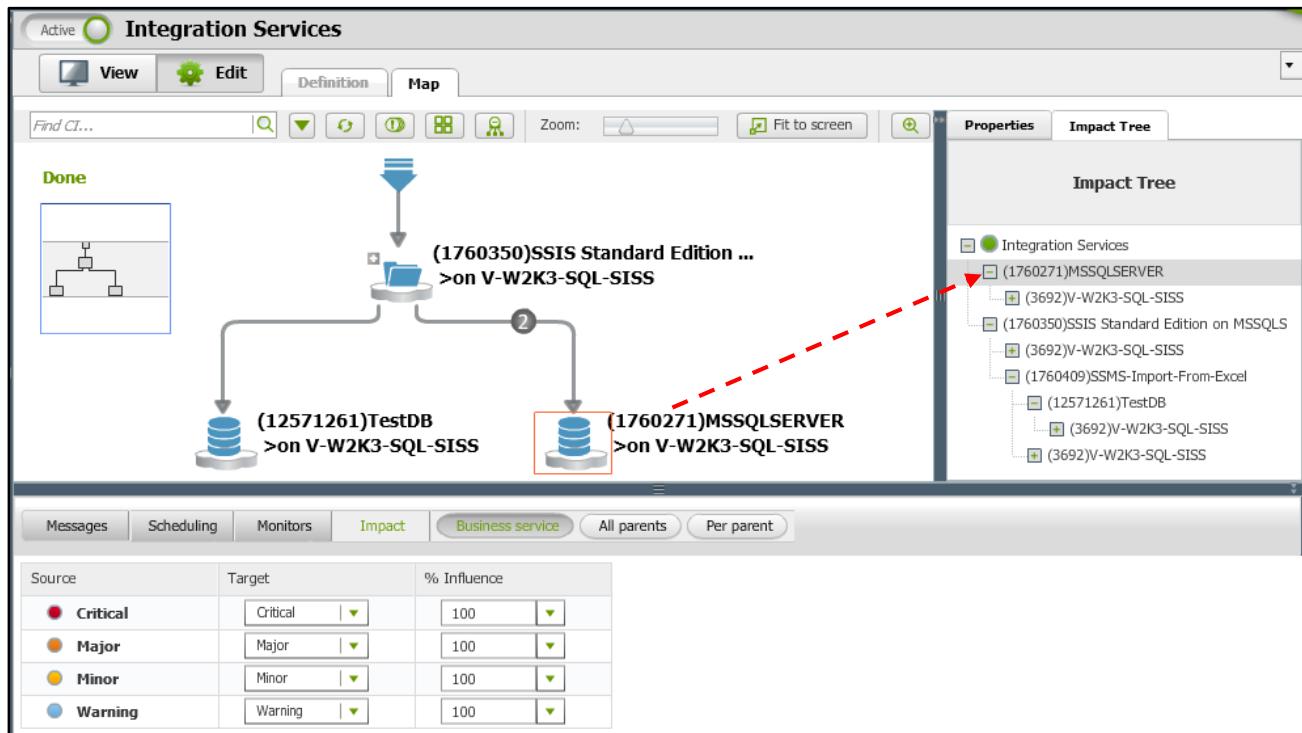
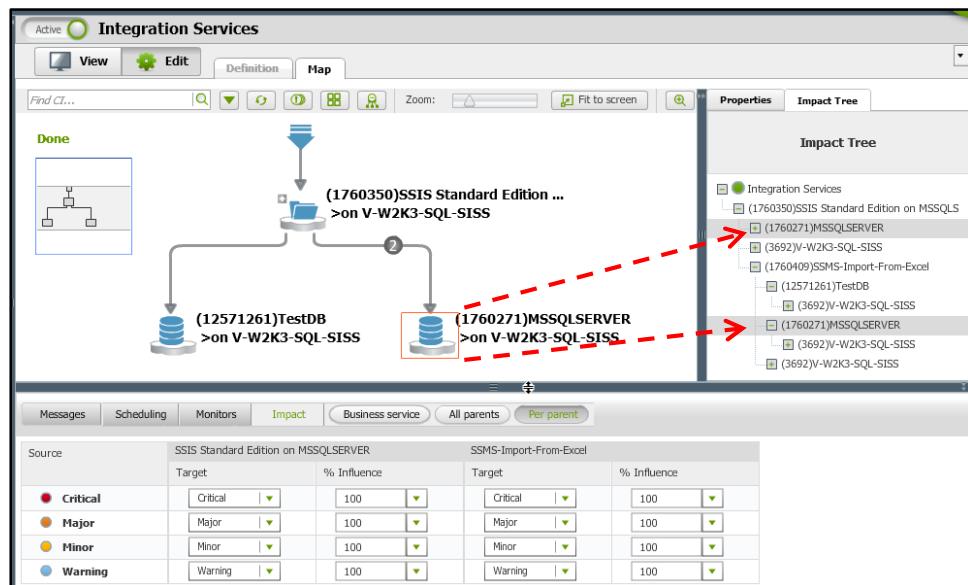


Figure 133: Per Parent Impact Tree for the same 2-parent object



## 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

Messages		Members' influence	Impact	
Member Status		Cluster Status	Members Value	
<input checked="" type="radio"/> Critical		Critical   ▾	<input type="radio"/> % Members :	<input checked="" type="radio"/> # Members :
<input type="radio"/> Major		Major   ▾	<input type="radio"/> % Members :	<input checked="" type="radio"/> # Members :
<input type="radio"/> Minor		Minor   ▾	<input type="radio"/> % Members :	<input checked="" type="radio"/> # Members :
<input type="radio"/> Warning		Warning   ▾	<input type="radio"/> % Members :	<input checked="" type="radio"/> # Members :

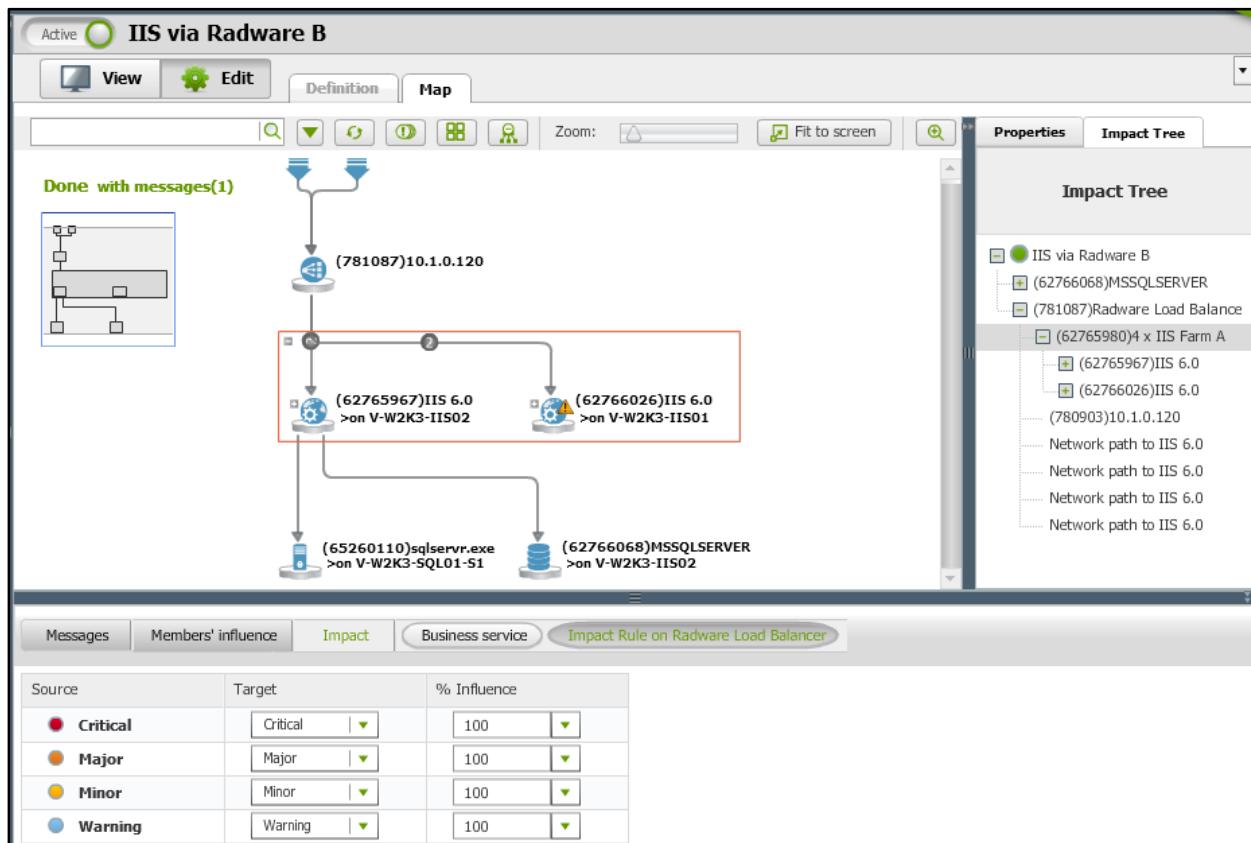
- If 20% of the members have a status of **Critical**, cluster status will be set to **Critical**.
- If 30% of the members have a status of Major, the cluster status will be set to **Major**.
- If 40% of the members have a status of Minor, the cluster status will be set to **Minor**.
- If 50% of the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

Figure 135: Cluster impact – Percentage of Members template

Messages		Members' influence	Impact	
Member Status		Cluster Status	Members Value	
<input checked="" type="radio"/> Critical		Critical   ▾	<input checked="" type="radio"/> % Members :	<input type="radio"/> # Members :
<input type="radio"/> Major		Major   ▾	<input checked="" type="radio"/> % Members :	<input type="radio"/> # Members :
<input type="radio"/> Minor		Minor   ▾	<input checked="" type="radio"/> % Members :	<input type="radio"/> # Members :
<input type="radio"/> Warning		Warning   ▾	<input checked="" type="radio"/> % Members :	<input type="radio"/> # Members :

- 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 [142](#).

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



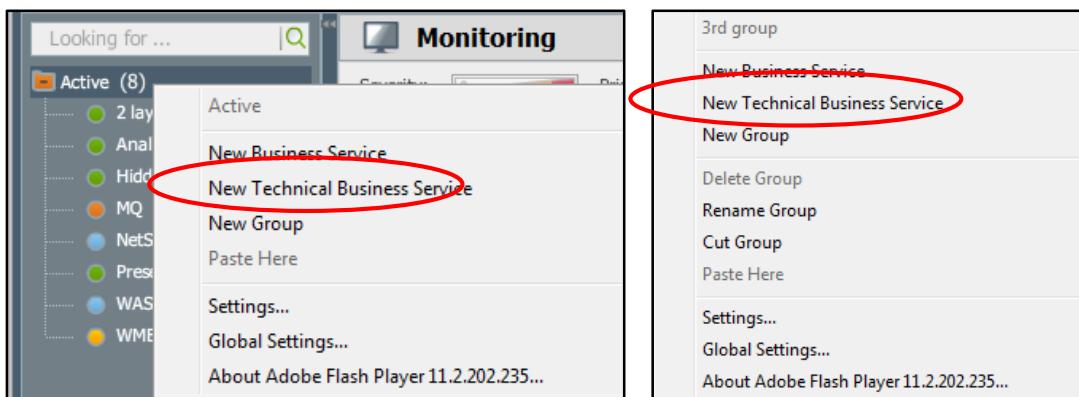
- When you finish defining Cluster Member and Cluster impacts, exit **Edit** mode. The changes you made are automatically saved

# Creating Technical Business Services

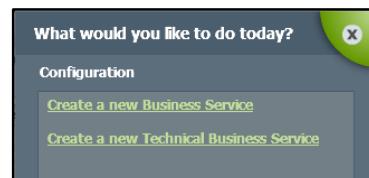
Technical business services are manual collections of objects. For example, to track the status of all Apache servers, you can define a technical business service called “Apache” and define a query that selects all Apache servers for that technical business service. The wizard that defines technical 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.



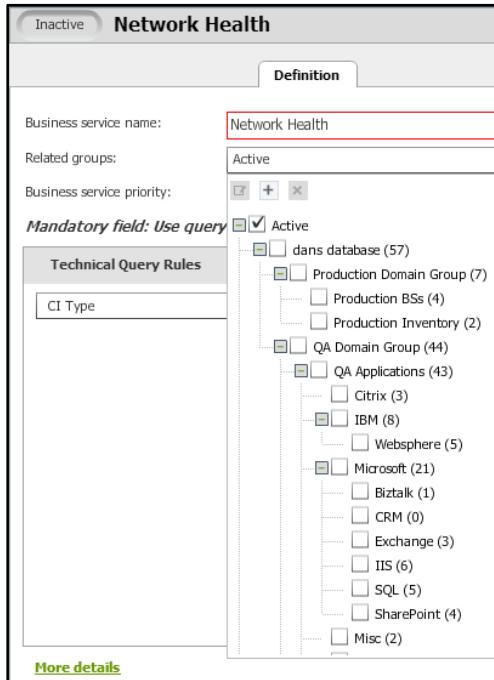
2. The Definition panel of the Technical Business Service wizard (FIGURE 138) is displayed.

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

The screenshot shows the 'Definition' panel of the Technical Business Service wizard. At the top, there are sections for 'Business service name' (with a red box around the input field), 'Related groups' (set to 'Active'), and 'Business service priority' (set to '5'). Below these is a note: 'Mandatory field: Use query parameters below to define the CI list'. A 'Technical Query Rules' section follows, containing a table with columns for 'CI Type', 'Equals', and '.NET Application'. There are also '+' and '-' buttons for adding and removing rules. At the bottom right of the panel is a 'Save and view Results' button.

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  icon, Add group  icon, 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**

The screenshot shows a dropdown menu for 'Business service priority' with the value '5' selected. Below the dropdown, a note says 'Select a value (low=1; high=5) from the Business service priority drop-down list'. At the bottom right of the dropdown area, there is an 'Add new query rule' button.

7. Click **Add new query rule** 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**

Mandatory field: Use query parameters below to define the CI list

Technical Query Rules		Add new query rule	
CI Type	Equals	.NET Application	+ <input type="button" value="X"/>
.NET framework version	Equals		+ <input type="button" value="X"/>
CI Type	Equals	.NET Application	+ <input type="button" value="X"/>
.NET framework version	Equals		+ <input type="button" value="X"/>
AND      OR			
<a href="#">More details</a>			
<input type="button" value="Save and view Results"/>			

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

- 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**

The screenshot shows four separate dropdown menus arranged in a grid:

- Top-left: CI Type (dropdown menu open, showing options like CI Type, Is Virtual Machine, Is Hypervisor, Application Processes.Process ID, Application Processes.Process Name, Application Services.Service Name)
- Top-right: Equals (dropdown menu open, showing options like Equals, Equals, Not Equals)
- Bottom-left: .NET framework version (dropdown menu open, showing options like .NET framework version, Alternate Label, Application Processes.Process ID, Application Processes.Process Name, Application Services.Service Name)
- Bottom-right: Equals (dropdown menu open, showing options like Equals, Equals, Not Equals, Start With)

- 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.

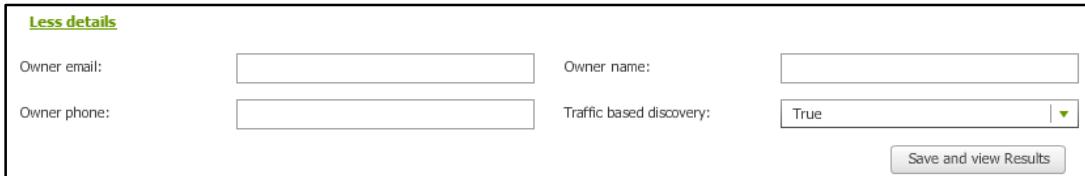
Next, do the following:

- If a relational operator drop-down list is displayed, select the relational operator.
  - Select (or fill in) the value that is to be matched.
  - If  is displayed **next** to a query line, click it to add an additional value to be matched.
- 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  .
  - 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.

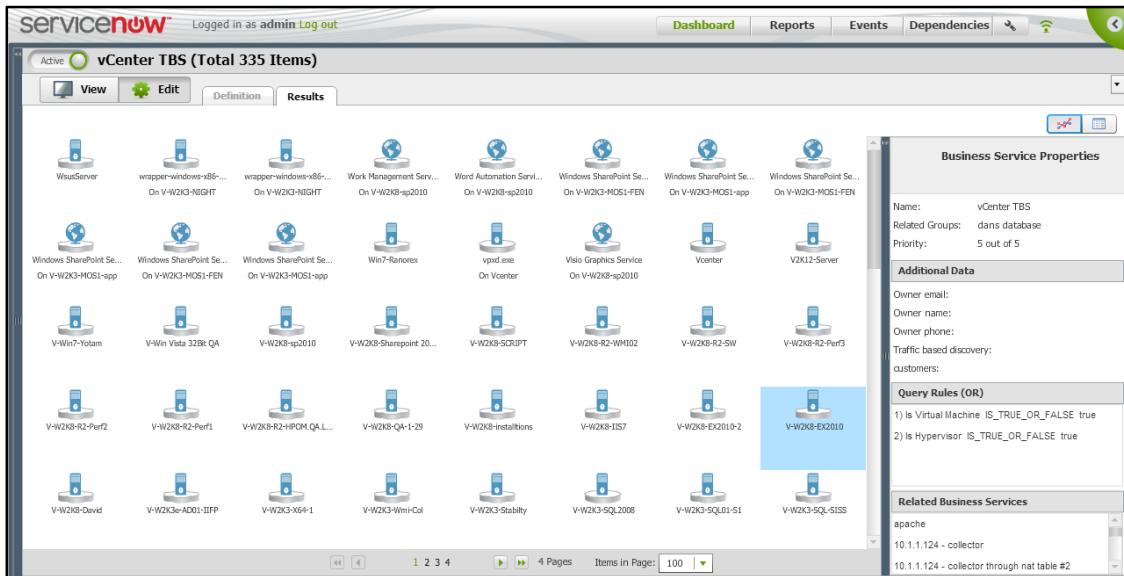
Figure 143: Technical Business Service – More details fields



The screenshot shows a configuration form for a Technical Business Service. It includes fields for Owner email, Owner name, Owner phone, and Traffic based discovery (set to True). A 'Save and view Results' button is at the bottom.

- 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



The screenshot shows the 'Results' panel for a 'vCenter TBS' search. It displays a grid of icons representing various business services. One item in the grid is highlighted. On the right, there is a sidebar titled 'Business Service Properties' with fields for Name, Related Groups, and Priority. Below this are sections for 'Additional Data', 'Query Rules (OR)', and 'Related Business Services'.

- 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.

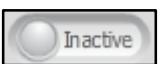
Figure 145: Technical Business Service – Results panel table display

CI Type	Name	Server
Host	WsusServer	
Generic Application	wrapper-windows-x86-32.exe	V-W2K3-NIGHT
Generic Application	wrapper-windows-x86-32.exe	V-W2K3-NIGHT
SharePoint Service	Work Management Service	V-W2K8-sp2010
SharePoint Service	Word Automation Services	V-W2K8-sp2010
SharePoint Service	Windows SharePoint Services Web Application	V-W2K3-MOS1-FEN
SharePoint Service	Windows SharePoint Services Web Application	V-W2K3-MOS1-app
SharePoint Service	Windows SharePoint Services Incoming E-Mail	V-W2K3-MOS1-FEN
SharePoint Service	Windows SharePoint Services Incoming E-Mail	V-W2K3-MOS1-app
SharePoint Service	Windows SharePoint Services Help Search	V-W2K3-MOS1-FEN
SharePoint Service	Windows SharePoint Services Help Search	V-W2K3-MOS1-app
Host	Win7-Ranorex	
Generic Application	vpxd.exe	Vcenter
SharePoint Service	Visio Graphics Service	V-W2K8-sp2010
Host	Vcenter	
Host	V2K12-Server	
Host	V-Win7-Yotam	
Host	V-Win Vista 32Bit QA	

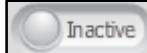
- Display the Element Properties of an object by clicking the object in either graph or table mode.

Figure 146: Technical Business Service – Element Properties

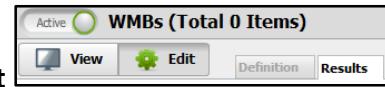
CI Type	Name	Server
Host	WsusServer	
Generic Application	wrapper-windows-x86-32.exe	V-W2K3-NIGHT
Generic Application	wrapper-windows-x86-32.exe	V-W2K3-NIGHT
SharePoint Service	Work Management Service	V-W2K8-sp2010
SharePoint Service	Word Automation Services	V-W2K8-sp2010
SharePoint Service	Windows SharePoint Services Web Application	V-W2K3-MOS1-FEN
SharePoint Service	Windows SharePoint Services Web Application	V-W2K3-MOS1-app
SharePoint Service	Windows SharePoint Services Incoming E-Mail	V-W2K3-MOS1-FEN
SharePoint Service	Windows SharePoint Services Incoming E-Mail	V-W2K3-MOS1-app
SharePoint Service	Windows SharePoint Services Help Search	V-W2K3-MOS1-FEN
SharePoint Service	Windows SharePoint Services Help Search	V-W2K3-MOS1-app
Host	Win7-Ranorex	
Generic Application	vpxd.exe	Vcenter
SharePoint Service	Visio Graphics Service	V-W2K8-sp2010
Host	Vcenter	
Host	V2K12-Server	
Host	V-Win7-Yotam	
Host	V-Win Vista 32Bit QA	

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.

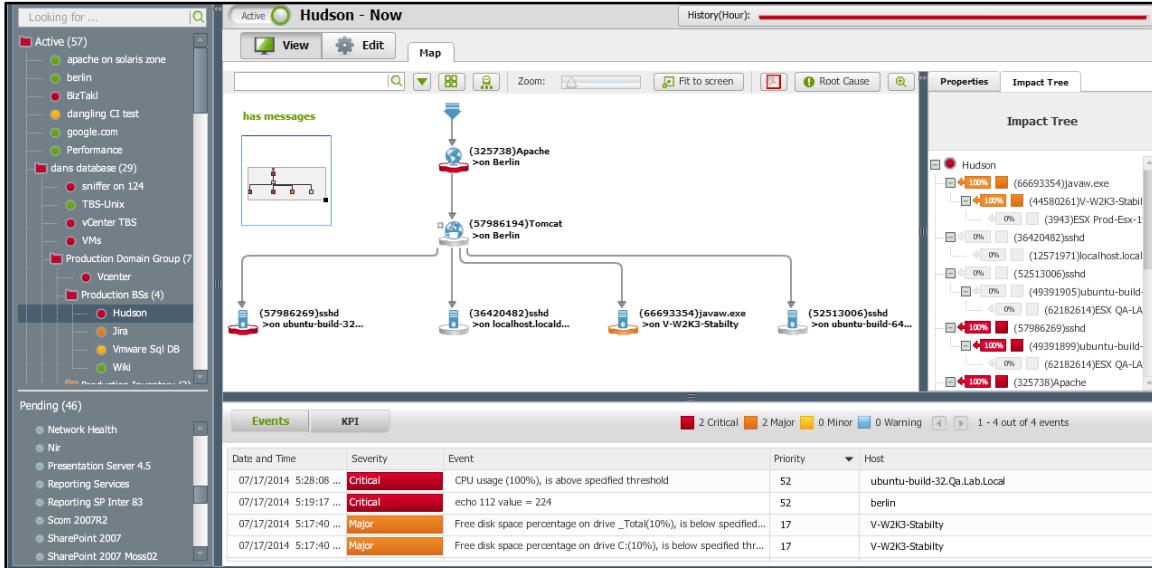
13. When the business service is , the **View/Edit** toggle buttons are displayed. Click **View** to view the **Results**. Click **Edit** to edit the **Definition** or **Results**.



# Root Cause Analysis

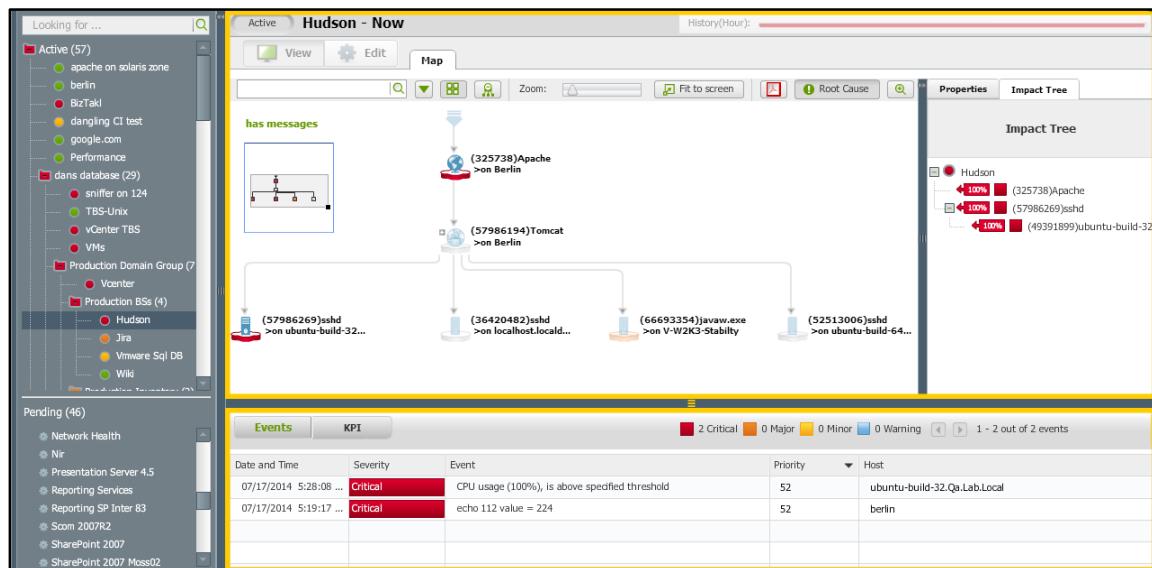
When a CI topology Map is displayed in **View** mode, click  to toggle into and out of **Root Cause** mode. When *not* in **Root Cause** mode, topology nodes are not grayed-out and all of the Element Properties, Events and KPIs can be displayed (Figure 147).

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 **KPIs** 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).

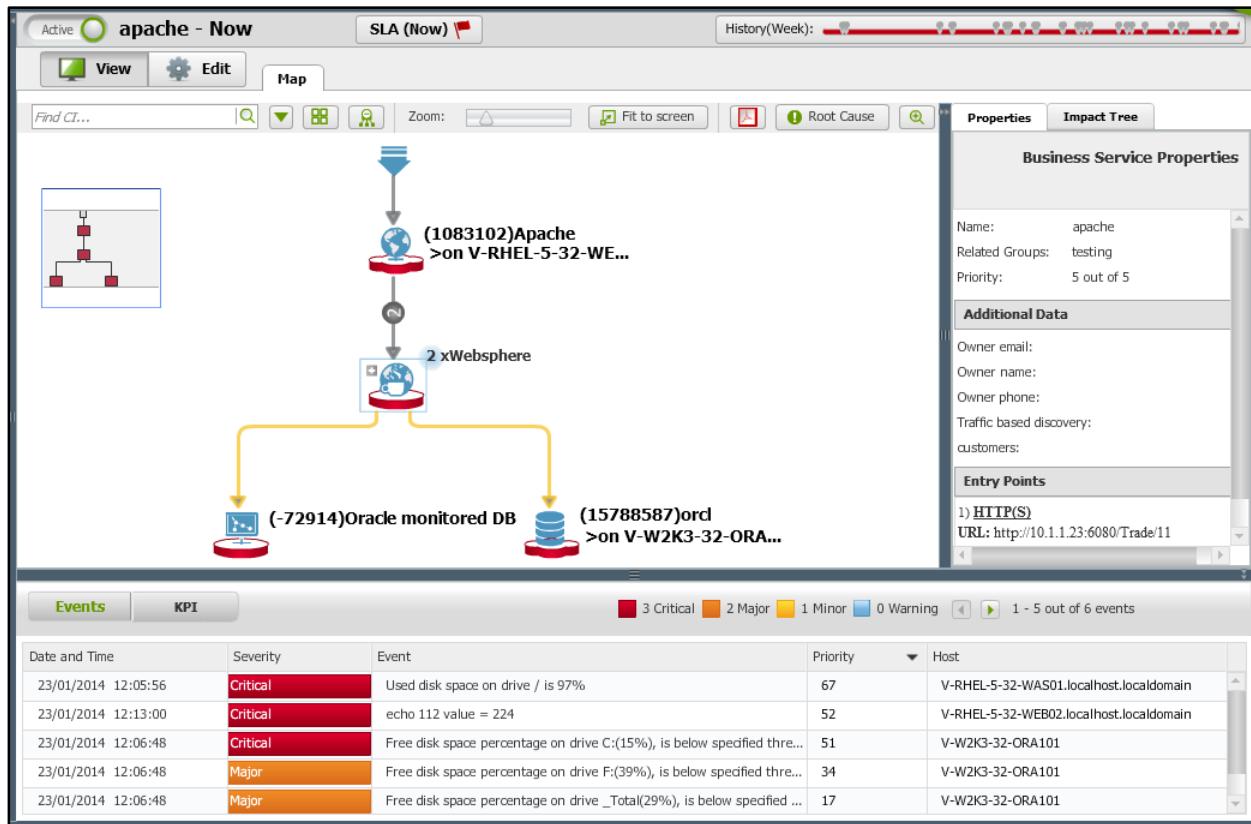
Figure 148: Topology Map and Impact Tree in Root Cause mode



# Business Service, Object or Connection Properties

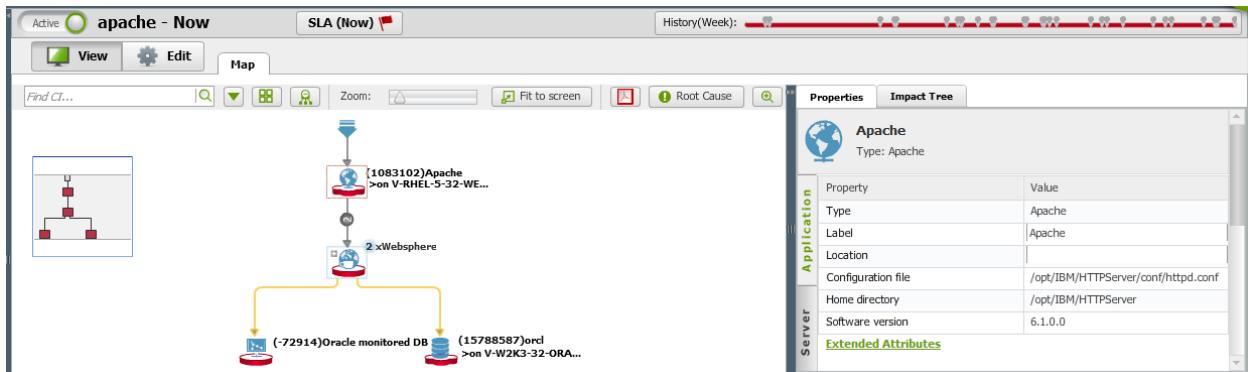
To view the properties of an active or inactive business service, click its topology Map background and then click the **Properties** tab in the top right pane. Its **Business Service Properties** are displayed.

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**

The figure consists of three side-by-side screenshots of a ServiceNow interface. Each screenshot shows the properties of an 'Apache' service. The tabs on the left indicate the type of technical business service:

- Application:** Shows properties like Address width (32), Label (V-RHEL-5-32-WEB02.localhost.localdomain), and Model (VMware Virtual Platform).
- Server:** Shows properties like VM cpu number (1), Hypervisor address (10.1.0.5), and VM image file ([QA on Netapp 02] V-RHEL-5-32-WEB02/V-RHEL-5-32-WEB02.vmx).
- VM:** Shows properties like VM memory mb (256), VM power status (poweredOn), and VM UUID (420cf19f-584a-1e1b-e882-1c873591f681).

Red dashed arrows point from the tabs to their respective property tables. A red arrow also points from the 'Server' tab to the 'VM' tab.

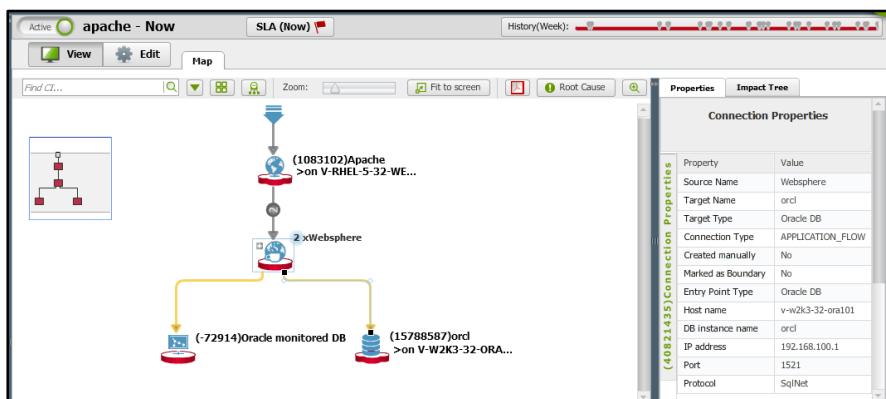
To display **complex Application, Server or Hypervisor** properties, click their **blue** or **green** underlined links. E.g., clicking **Ports** in the **Server** properties panel will display a **Ports** table.

**Figure 152: Technical Business Service – Ports table**

Ports									
Apache									
caption	card_caption	card_identifier	description	hw_address	internal_port_id	parent_port_identifier	port_identifier	state	type
eth2	---	---	---	00:50:56:8C:26:D8	67077010	---	eth2	---	---
eth1	---	---	---	00:50:56:8C:1E:CB	67077009	---	eth1	---	---
eth0	---	---	---	00:50:56:8C:4F:F0	57987108	---	eth0	---	---

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.

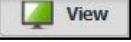
**Figure 153: Connection Properties panel**



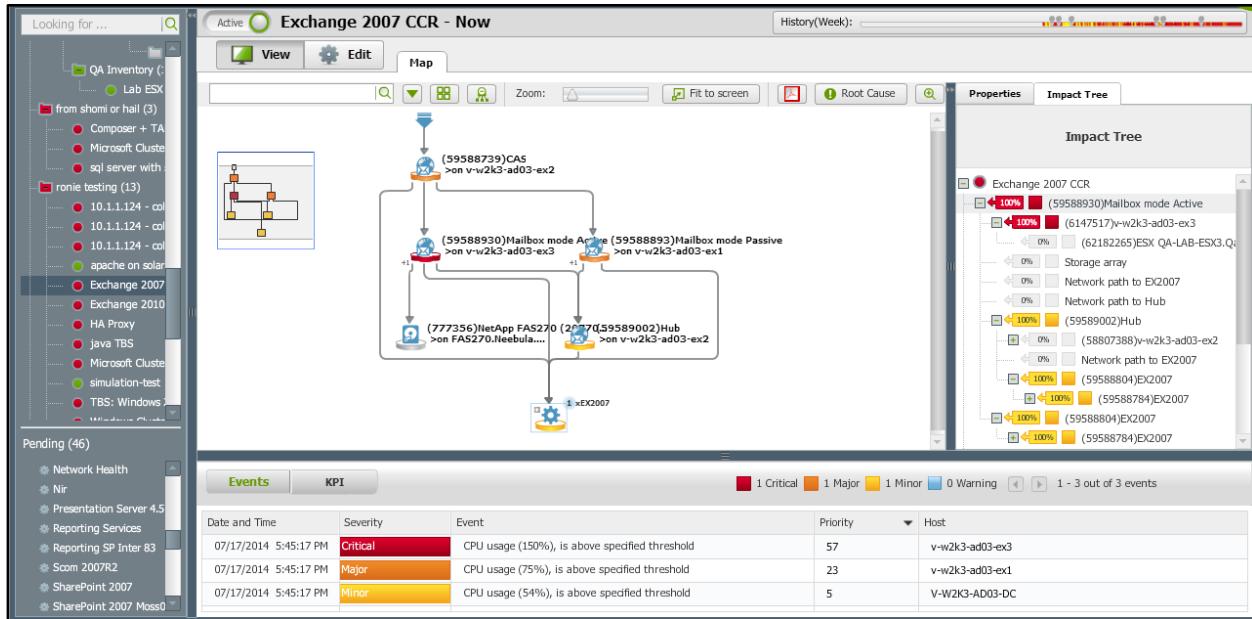
## Viewing the Impact Tree of a Business Service

As described in [DEFINING THE IMPACT OF AN OBJECT ON ITS PARENT OR BUSINESS SERVICE](#) on page 142, 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**



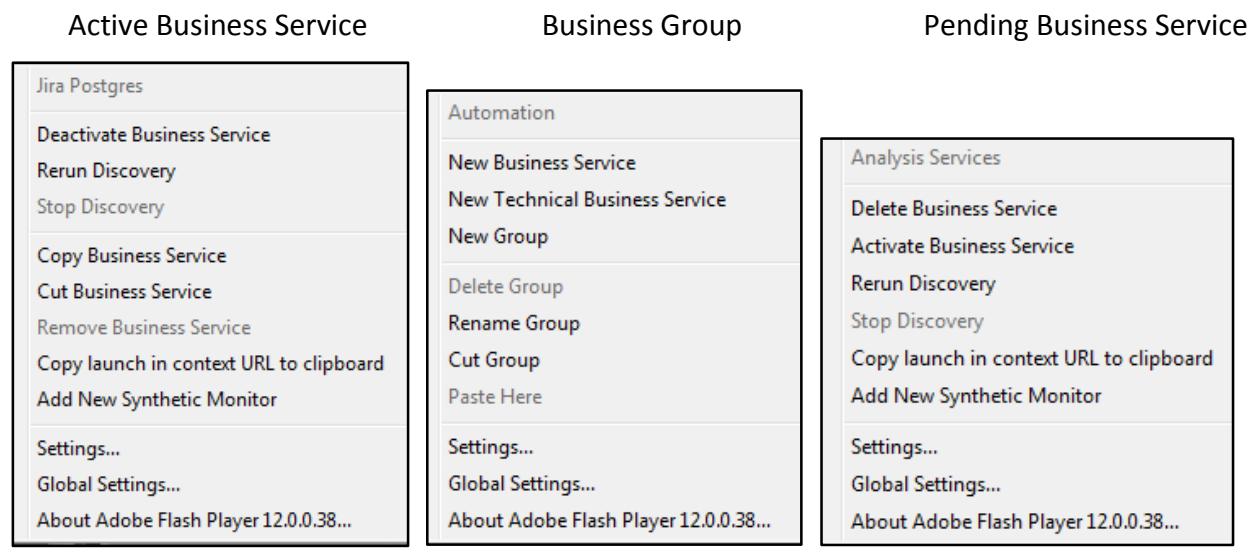
In the **Impact Tree** panel, the color of the circle indicates the Severity level of the Business Service. The color of each square indicates the Severity level of that component. The color of each  symbol indicates the Severity level and percentage effect of that component on its parent.

# 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**



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

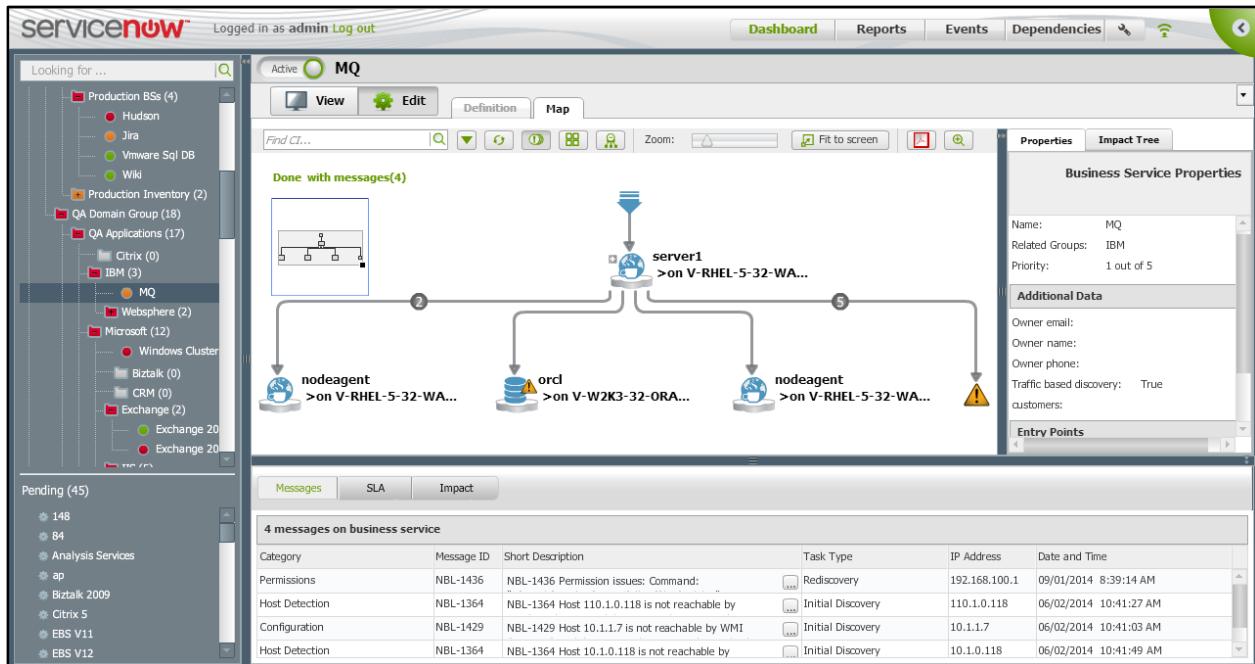
# Editing a Business Service

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.

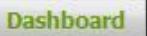
## Topology Map

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

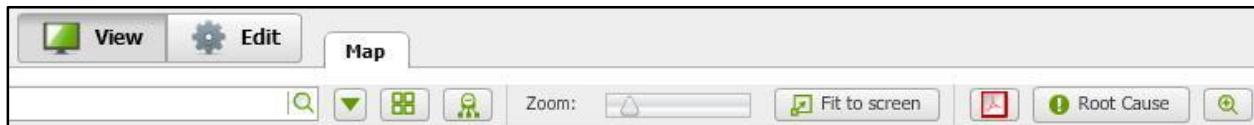


Figure 158: Map manipulation icons in Edit mode



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

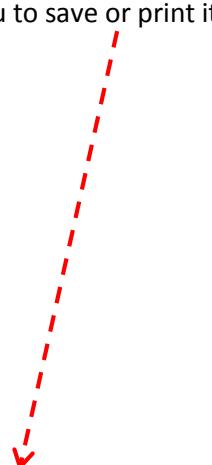
Table 8: Topology Map manipulation actions

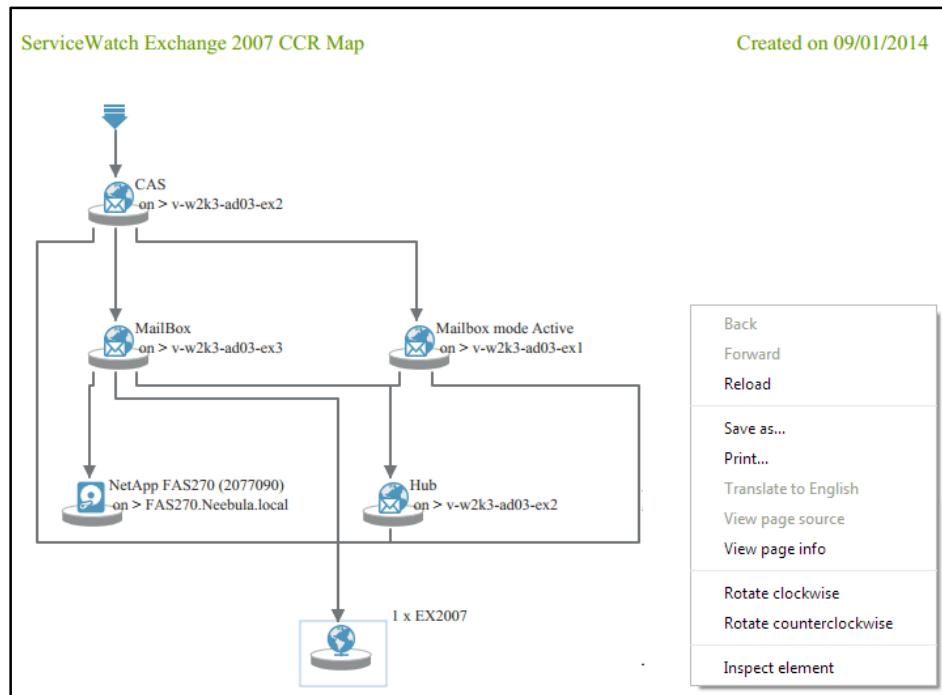
Desired Action	Relevant Icon	How to do it
To group undiscovered CIs and messages by source CI		In <b>Edit</b> mode, click this icon. To re-display the original Map, click this icon again.
To gray-out all CI icons except the root cause CI		In <b>View</b> mode, click the <b>Root Cause</b> button. Click it again to see the usual display.
To refresh the topology Map display		In <b>Edit</b> mode, click the <b>Refresh</b> button.
To list only CIs that contain the specified text string in the <b>Active and Pending</b> panels		Type the string in the Search text box.  is <i>not</i> clickable.
To display the Network Path for a connection between components	(no icon)	Right click the connection and select <b>Show network path</b> in the pop-up menu. <b>Network Path &amp; Map</b> functionality are similar. See <a href="#">CHAPTER 10: MONITORING NETWORKS</a> .
To adjust the size of the icons in the display		Move the <b>Zoom</b> slide at the top of the screen.
To set the display size to fit the screen		Click the <b>Fit to screen</b> button

Desired Action	Relevant Icon	How to do it
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.
To hide/display the overview thumbnail		Click the <b>Overview</b> 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 <b>Magnifier</b> 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	 <input checked="" type="checkbox"/> Remove connections between siblings	Click  and select/clear the checkbox. Connections are only hidden and <i>not</i> disconnected.
Export a map		In <b>View</b> 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 PROCESSING FLOW
  - ✓ INFORMATION TRANSFER OF EMS EVENTS TO SERVICEWATCH
  - ✓ SERVICEWATCH PREDEFINED EVENT FIELDS
  - ✓ INTEGRATING SERVICEWATCH WITH YOUR EMS
    - EVENT RULES BY SOURCES TREE
    - UNBOUND EVENTS TABLE MODES
- DEFINING THE EVENT COMMAND LINE
- MAPPING EMS FIELDS TO SERVICEWATCH FIELDS
- EXTRACTING AND BINDING EVENT INFORMATION
  - ✓ CONCEPTS
  - ✓ DEFINE THE BINDING RULE FOR AN EVENT
    - Defining rows in the Event Fields Rules table
    - Defining rows in the Advanced Rule Binding Definition table
  - ✓ DISPLAYING THE DETAILS OF AN EVENT IN THE UNBOUND EVENTS

## Displaying Events

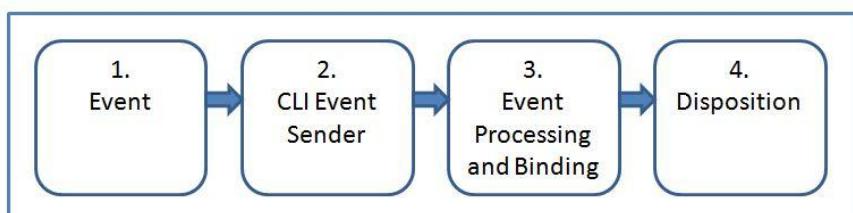
Event Management Systems (EMSs) monitor computer networks and detect significant events. These events may trigger alerts (e.g., SMSs) and be displayed by the EMS application.

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:{0}.
  - ✓ 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**

<b>Note</b>	<b>Predefined Field</b>	<b>Description</b>
	<b>businessServiceName</b>	Business service name
	<b>ciTypeName</b>	CI type name
*	<b>emsSystem</b>	EMS system that sent the event
	<b>expireTime</b>	Time at which the event is no longer relevant
	<b>hostAddress</b>	Host name or IP of the CI to which event should be bound
**	<b>messageKey</b>	Unique identifier for a message. When a new event with the same messageKey arrives, the old active event is closed.
	<b>ownerID</b>	Owner name or ID
	<b>resolutionState</b>	Event resolution state. Values: NEW,CLOSED
**	<b>severity</b>	Event severity: INFORMATION, WARNING, MINOR, MAJOR, CRITICAL
	<b>state</b>	Event state. Values: UNKNOWN, NOT OWNED, OWNED, ACKNOWLEDGED, DELETED
	<b>text</b>	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{0}.

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.

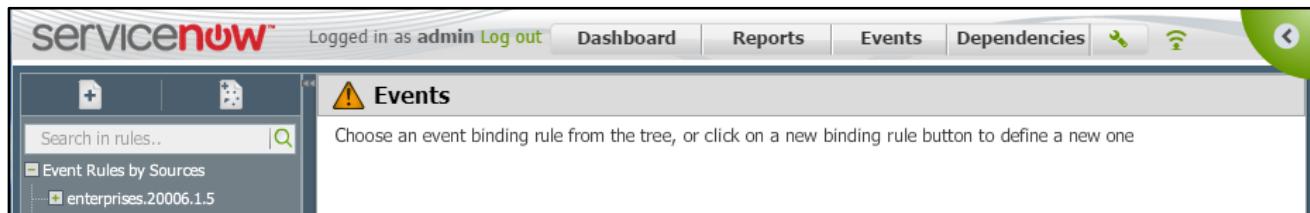
- ✓ Extracted information that can be mapped to object attributes helps determine the configuration item type to which the event relates, which in turn helps ServiceWatch bind the event to the configuration item (CI).
- ✓ Other extracted data mapped to event fields can provide ServiceWatch with useful 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  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

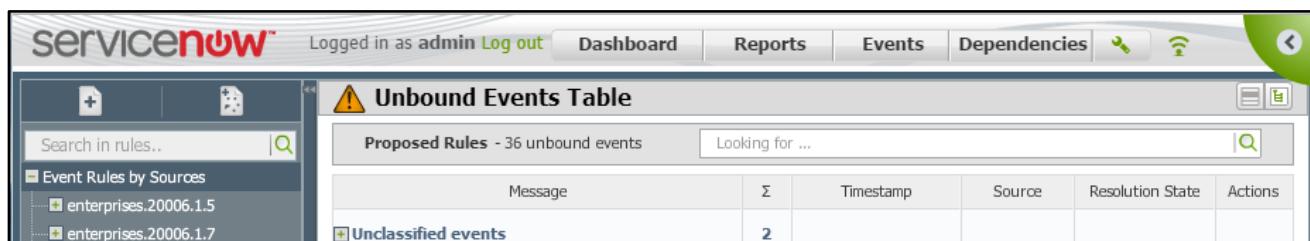


Figure 162: Unbound Events Table in Tabular mode



**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](#)

Message	$\Sigma$	Timestamp	Source	Resolution State	Actions
<b>Host [1] usage - Metric [2] Usage = [3] on ESX: [4]</b>	3				
Host memory usage - Metric Memory Usage = 88% on ESX: 172.16.1.15		Dec-26-2...	vmwVC	NEW	
Host memory usage - Metric Memory Usage = 89% on ESX: 10.1.0.10		Dec-26-2...	vmwVC	NEW	
Host cpu usage - Metric CPU Usage = 74% on ESX: 10.1.0.10		Dec-26-2...	vmwVC	NEW	
<b>Virtual machine cpu usage - Metric CPU Usage = [1] on VM: V-W2K3-R2-SQL01-S01</b>	3				
Virtual machine cpu usage - Metric CPU Usage = 100% on VM: V-W2K3-R2-SQL01-S01		Dec-26-2...	vmwVC	NEW	
Virtual machine cpu usage - Metric CPU Usage = 99% on VM: V-W2K3-R2-SQL01-S01		Dec-26-2...	vmwVC	NEW	

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 <ServiceWatchServer>\event\_cli\bin\

**On Unix:** **nblevent** is a shell script in the path <ServiceWatchServer>/event\_cli/bin/

To see 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 <*ServiceWatchServer*>/event\_cli/conf/

## Mapping EMS Fields to ServiceWatch Fields

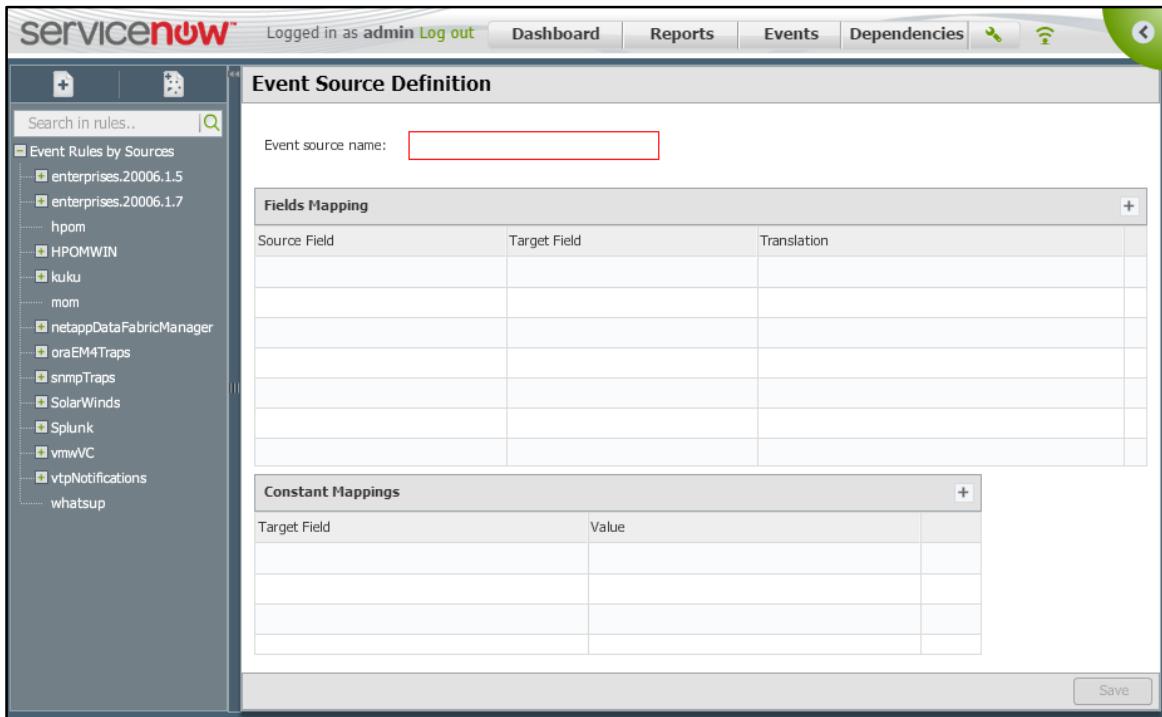
If EMS fields use different field names and/or values than those used by corresponding ServiceWatch fields, you must map the EMS field and its values to the corresponding ServiceWatch field and values. **vCenter** and **MOM** fields are already mapped in ServiceWatch. For other EMS applications, you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

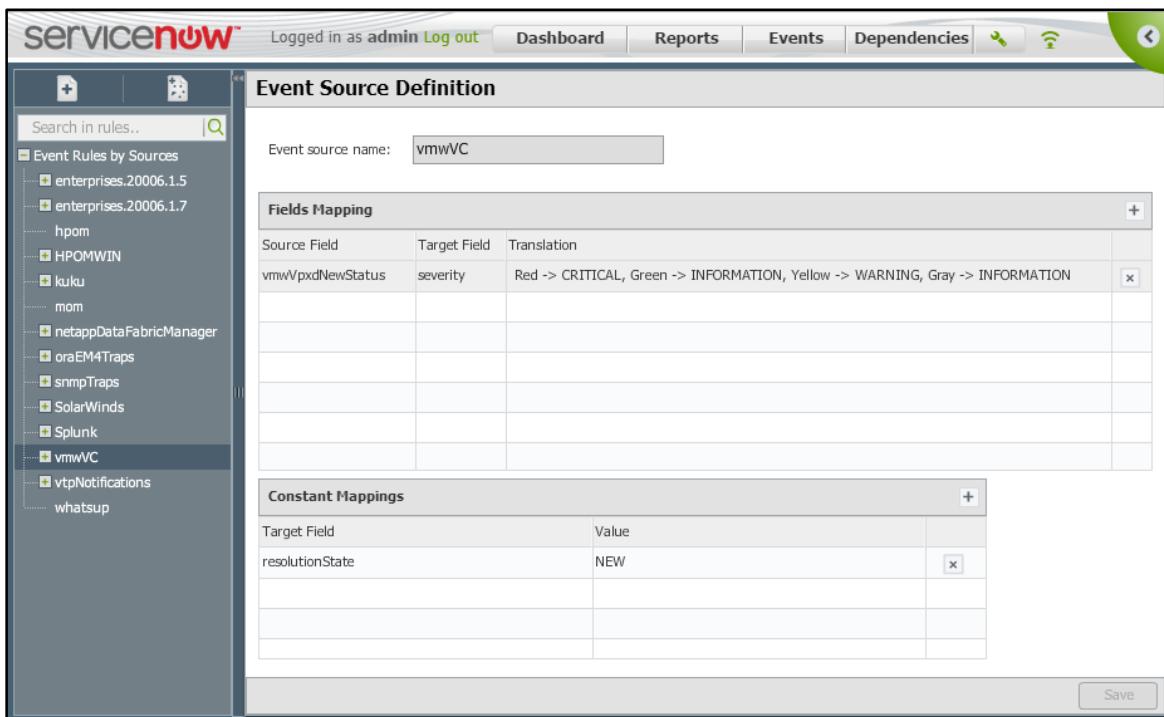
1. Click the Event Sources/Rules option of the  Settings drop-down menu.
2. Click the New Event Source  icon at the top of the Event Rules by Sources tree. An empty Event Source Definition window (Figure 164) is displayed.

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



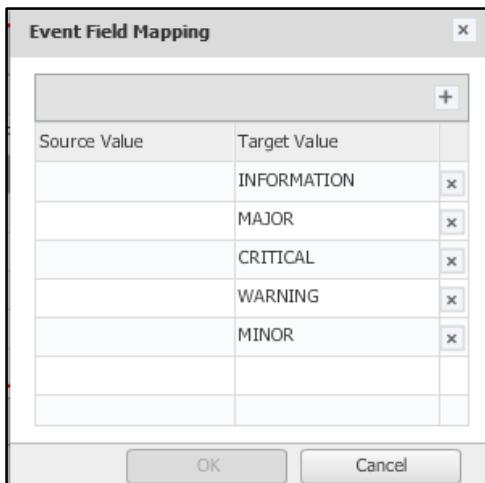
**Note:** To display or modify an existing Event Source Definition, click that definition (at level 1) in the **Event Rules by Sources** tree.

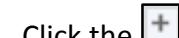
4. Select the (level 1) **Event source name** in the tree (for example, **vmwVC**). It is automatically inserted in the **Event source name** field.

5. Map EMS fields and values to ServiceWatch fields and values by doing the following for each EMS field to be mapped:

- 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.
- The first value in the **Target Field** drop-down list is automatically entered in the **Target Field**.
- Click the **Source Field** to select or specify the name of the EMS field being mapped.
- Click the **Target Field** to select the corresponding ServiceWatch field from its drop-down list.
- 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



- 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  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:
- 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.
  - In the **Target Field** column, specify the name of the EMS field that will be assigned the constant value.
  - In the **Value** column, specify the constant value for that EMS field.
7. When you have finished the **Event Source Rules** definition, click the  button. The event source rule is added to the system.

# Extracting and Binding Event Information

This section contains the following topics:

- [Concepts](#)
- [Define the Binding Rule for an Event](#)
- [Displaying the details of an event in the Unbound Events](#)

## 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:

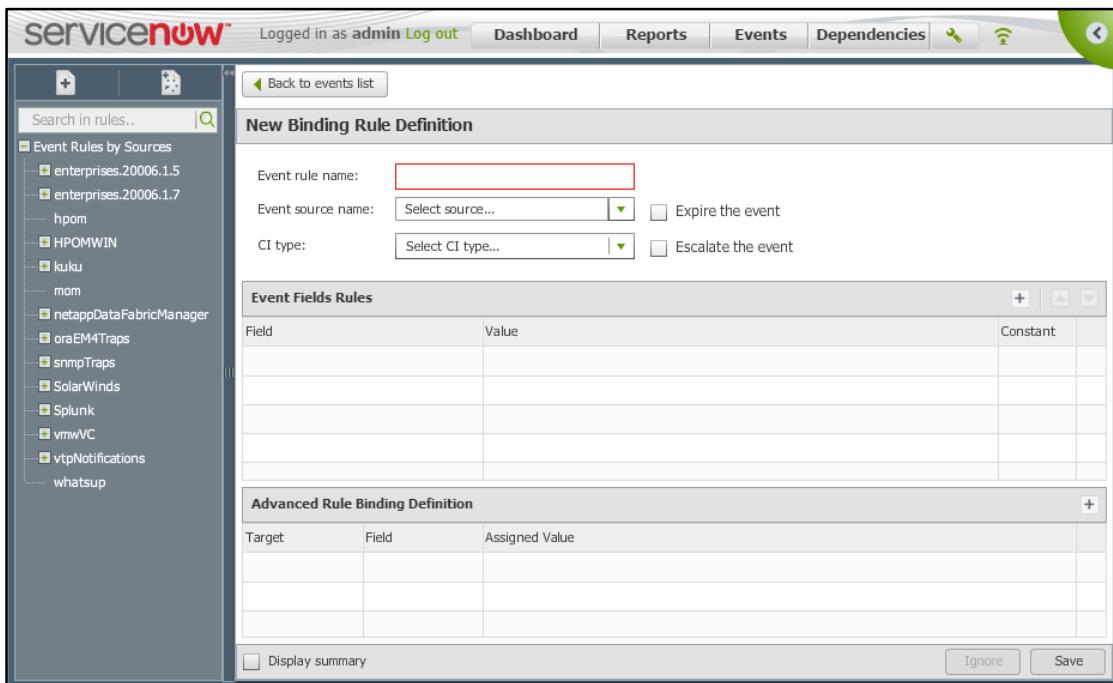
- To search for an event in either mode, enter a search string in the Looking for **Search** field above the table.
- You can scroll up or down in either mode by using the vertical slide bar.
- In either mode, you can display the details of an unbound event by right-clicking the event row and selecting **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 when finished to cause messages that match the definition to be bound to the appropriate configuration item.
- Click 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 to leave the event unbound or click to cause messages that match the definition to be ignored and permanently discarded. If you click , 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](#)

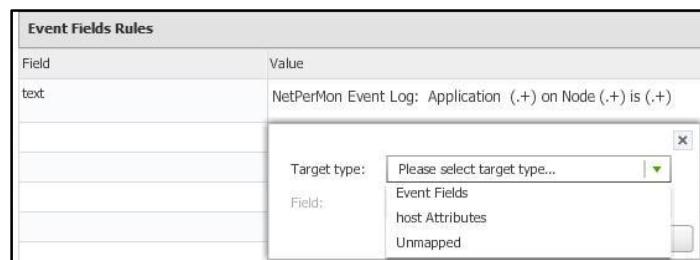
The screenshot shows the 'Binding Rule Definition' page in ServiceNow. The top navigation bar includes 'Logged in as admin Log out', 'Dashboard', 'Reports', 'Events', 'Dependencies', and other icons. On the left, a sidebar titled 'Event Rules by Sources' lists various sources like 'enterprises.2006.1.5', 'enterprises.2006.1.7', 'hpom', 'HPOMWIN', 'kuku', 'mom', 'netappDataFabricManager', 'oraEM4Traps', 'snmpTraps', and 'SolarWinds'. Under 'SolarWinds', there's a 'host' category expanded, showing items such as 'Application Status', 'Component\_Status', 'ComponentOnAppStatus', 'Counter is up', 'Counter status', 'Group Status', 'Group status 1', 'Group status down', 'Host not responding', and 'Interface High Transmit'. The main panel has three sections: 'Binding Rule Definition' (Event rule name: 'Application Status', Event source name: 'SolarWinds', CI type: 'host'), 'Event Fields Rules' (a table with one row: Field 'text' and Value 'NetPerMon Event Log: Application +(.) on Node (.+) is (.+)'), and 'Advanced Rule Binding Definition' (a table with one row: Target 'Event Fields', Field 'messageKey', Assigned Value '\$networkNodeId+"\_"+\$netObjectId+"\_"+\$app+"\_app\_status"'). At the bottom are 'Display summary', 'Ignore', and 'Save' buttons.

### 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.

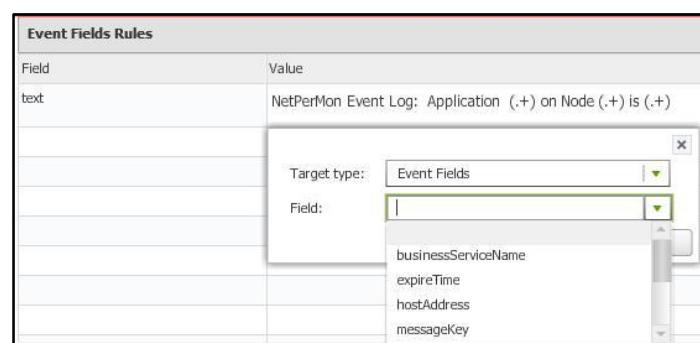
- The **Field** and **Value** columns identify source fields. Each source field has its own row in the table. If you are defining a rule for an existing unbound event, these fields are populated with information from the event.
  - Holding the hand-cursor over a constant or variable in the **Value** 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:
    - a. Click the + button in the header of the **Event Fields Rules** table to add an empty row.
    - b. In the **Field** column, specify the field type.
    - c. In the **Value** column, specify the value to be returned by the event.
    - d. 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.

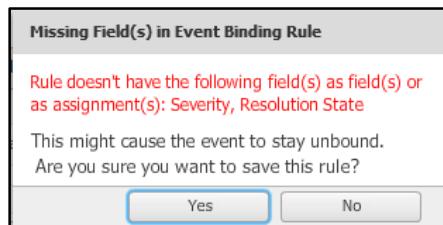
5. After you finish steps 2 through 4, perform the steps described in [Defining rows in the Advanced Rule Binding Definition table](#) on page [179](#) if and only if one or more target fields specified in steps 2 through 4 must be changed to a value other than the **Value** displayed in the **Event 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**

Timestamp	Source	Message	Resolution State
Feb-07-2014 16:50	NEEBULA	SQL latency is 78	NEW
Feb-07-2014 16:49	NEEBULA	SQL latency is 546	NEW
Feb-07-2014 16:48	NEEBULA	SQL latency is 343	NEW
Feb-07-2014 16:39	NEEBULA	SQL latency is 89	NEW

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 or button in **Tabular** mode, or the button.
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 or in **Tabular** mode or click ,
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 to close the **Event Details** table.[{0}](#).

**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](#)

Key	Value
Ems System	test
Text	Ping not returned
Severity	MINOR
Unbound reason	Event bound to host
ID	67030052
Message Key	6
Event Creation Time	20/01/2014 16:48:38
Neebula Event Time	20/01/2014 16:48:38
Host Address	172.16.1.3
hwAddr	00:50:56:8C:00:FE
Priority	0

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
  - ✓ Severity Color Coding
  - ✓ Event Priority
  - ✓ Viewing All Business Service Statuses at a Glance
  - ✓ Tile Dashboard
  - ✓ Bubble Dashboard
- View a Business Service or CI
- MODIFYING MONITOR ATTRIBUTES
- AGGREGATE MONITORS
- SYNTHETIC MONITORS
- KPIs (KEY PERFORMANCE INDICATORS)

## 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.

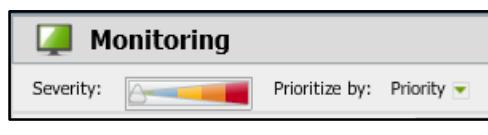
Note: The bottom pane also has a KPI (Key Performance Indicators) panel. This panel is discussed in [KPIs \(Key Performance Indicators\) on page 194](#).

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 **Dashboard** 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.{0}.

## 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.

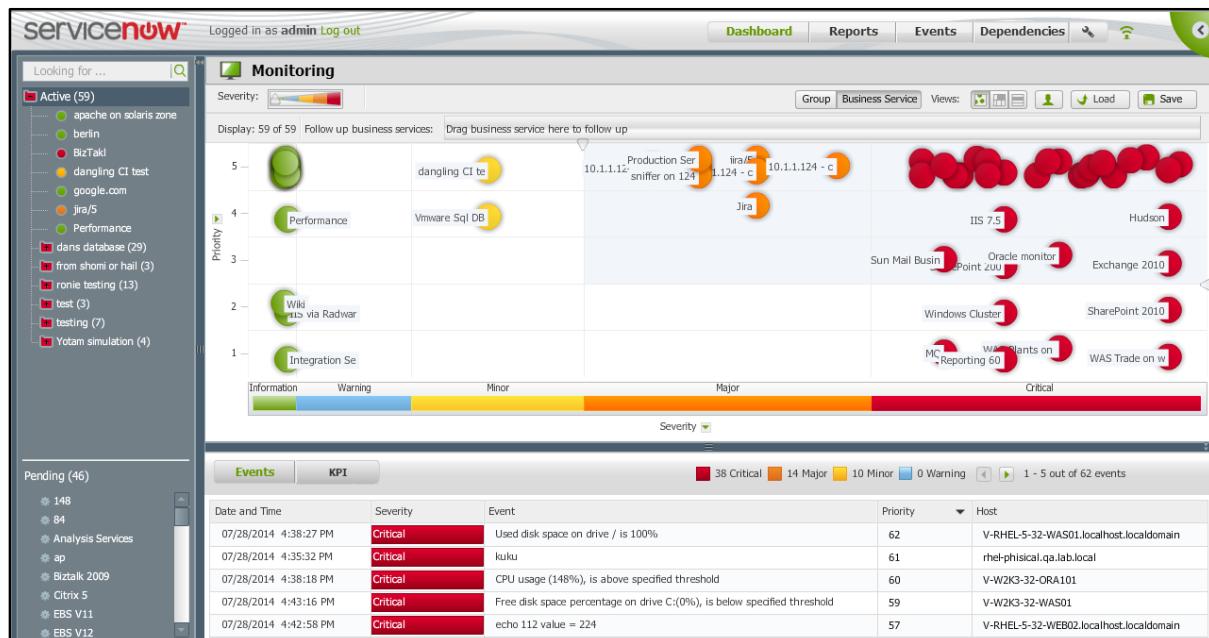
**Figure 174: Tile Dashboard**



## 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

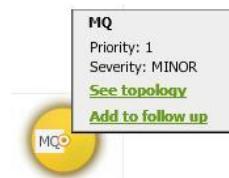
For information about this Dashboard, see [List Format Dashboard](#) on page 48.

## 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.

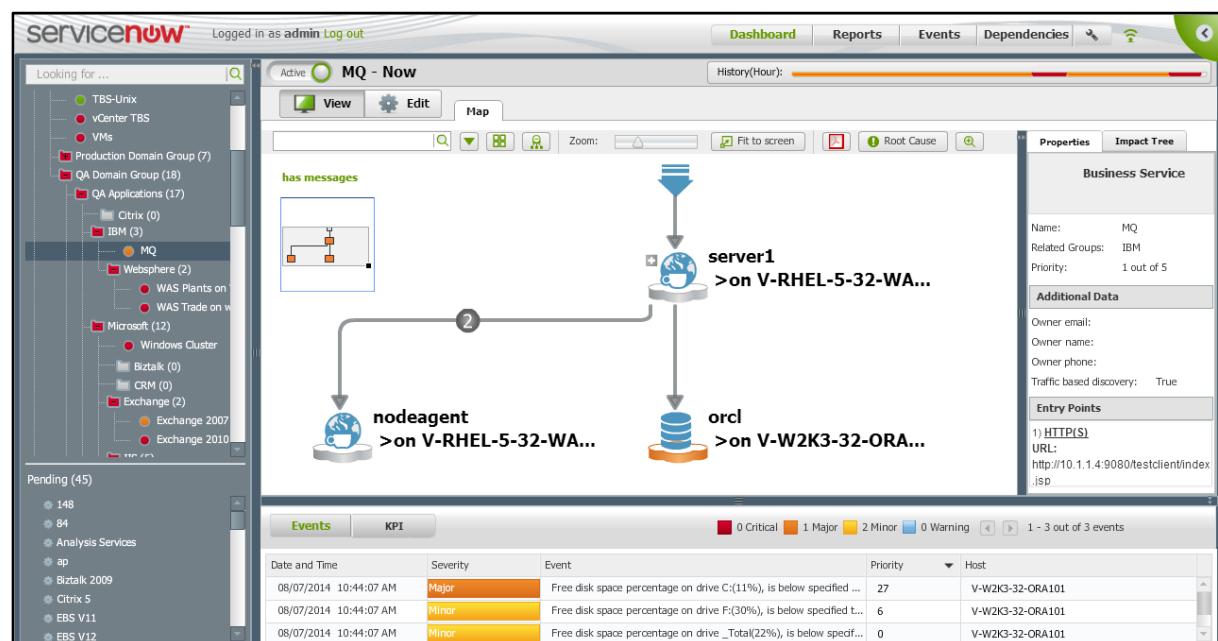
[Figure 176: Bubble tool tip](#)



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.[\[0\]](#)

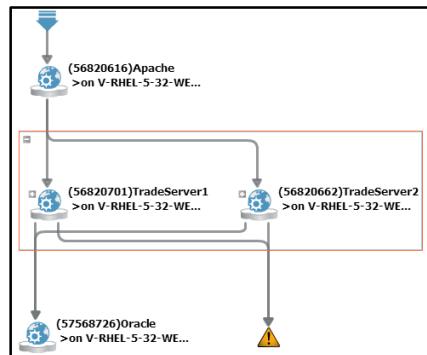
## Map Panel

[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 161.
- To change or fix the topology, click  **Edit**. For details, see [ADJUSTING THE BUSINESS SERVICE TOPOLOGY](#) on page 137.
- 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 156).
- 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.

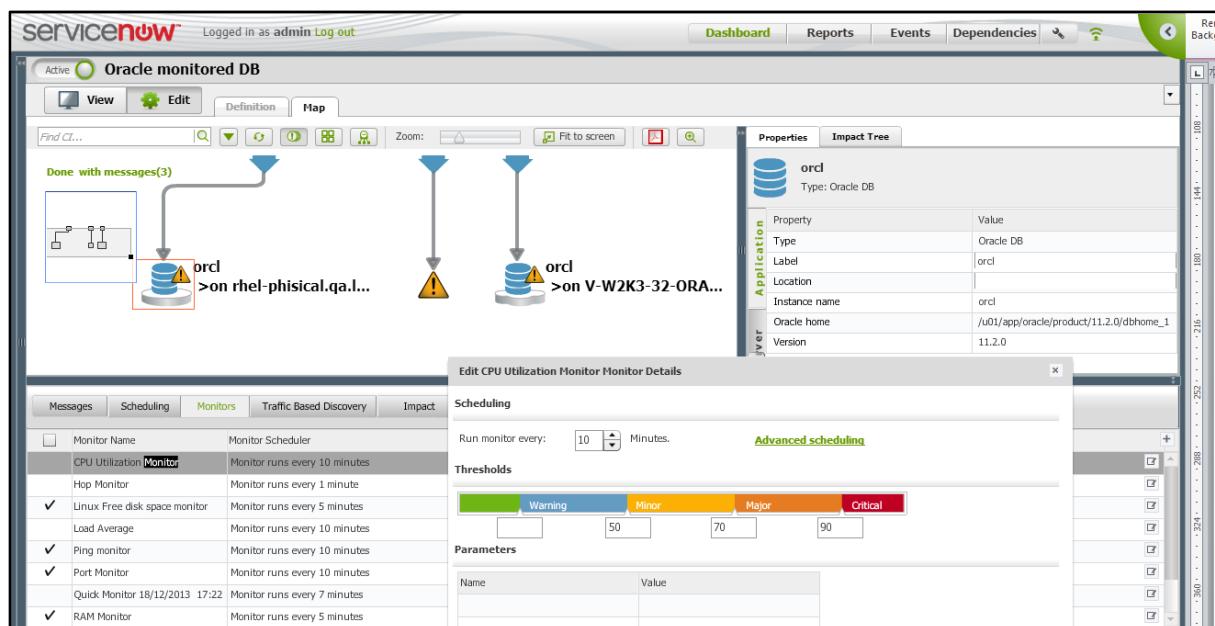
**Figure 178: All Groups & Business Services tree**



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**

Check Monitor Results - Events List	
Event Text	Severity
Result is 57.0	INFORMATION

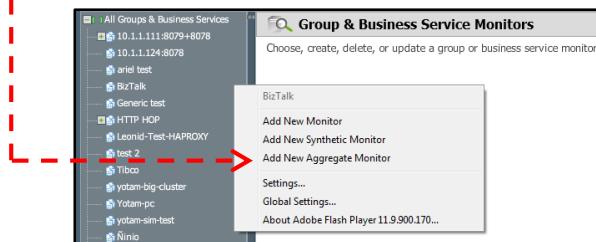
Click  to exit without saving changes. Click  to delete the monitor.

# 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

The screenshot shows the 'Exchange 2014 Max' monitor configuration page. On the left, a sidebar lists 'All Groups & Business Services' with many entries like 'apache on solaris zone', 'Avi Test 1', 'berlin', etc. The main panel has sections for 'Scheduling' (set to run every 10 minutes, every day, including Sunday through Saturday), 'Content' (with a dropdown for selecting monitors to aggregate, currently showing 'Hop Monitor'), and 'Result' (with a threshold slider set at 60, 75, and 90). A red box highlights the 'Maximum' radio button under 'Please select an operation'.

Click  to save the new aggregate monitor.

Click  to generate monitor output, for example:

Figure 183: Check Monitor Results – Events List

Check Monitor Results - Events List	
Event Text	Severity
Result is 57.0	INFORMATION

Click  to exit without creating or saving changes.

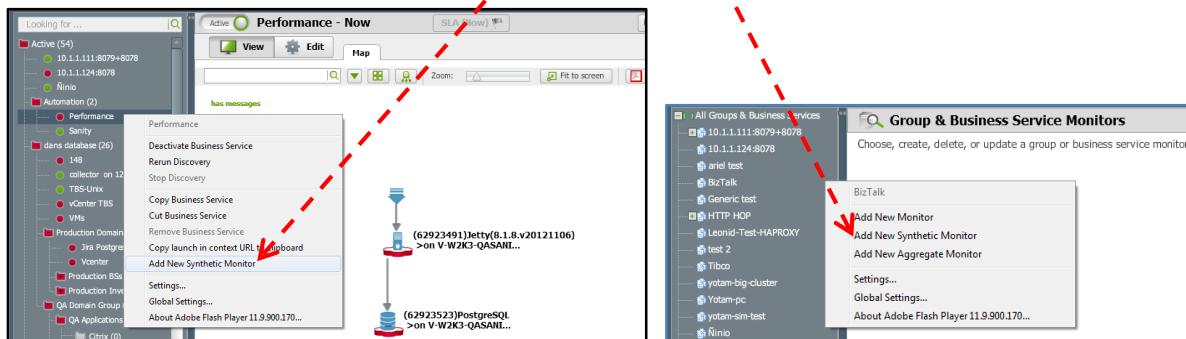
Click  to delete an existing aggregate monitor.

## 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.

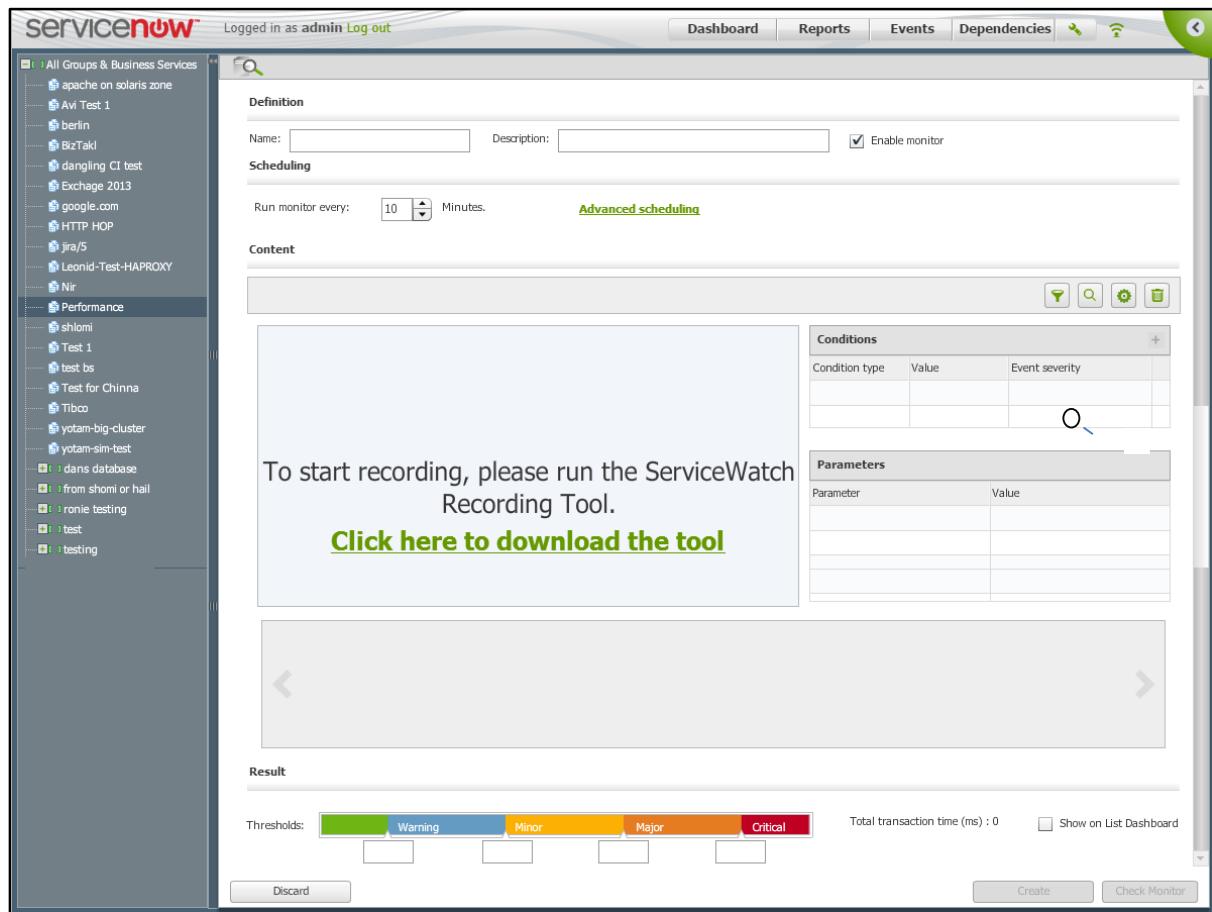
To add a synthetic monitor to a business service, right-click that business service in the **Active or Pending** Dashboard tree and select the **Add New Synthetic Monitor** option in the pop-up menu or click , click the **Group & Business Service Monitors** option, right-click a Business Service in the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

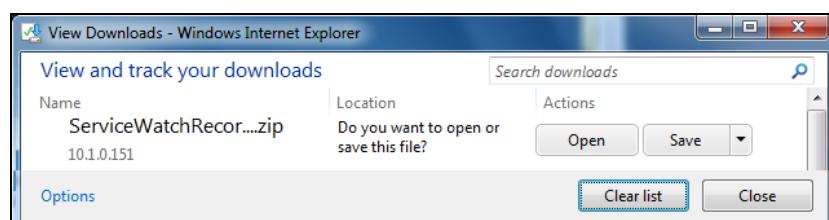
Click the Recording Tool link ([Click here to download the tool](#)) only once for each ServiceWatch client machine to download a zip file containing a **MinHook.x86.dll** file, a **params.ini** file and a **ServiceWatchRecorder.exe** file. Different download dialog boxes are displayed by Internet Explorer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

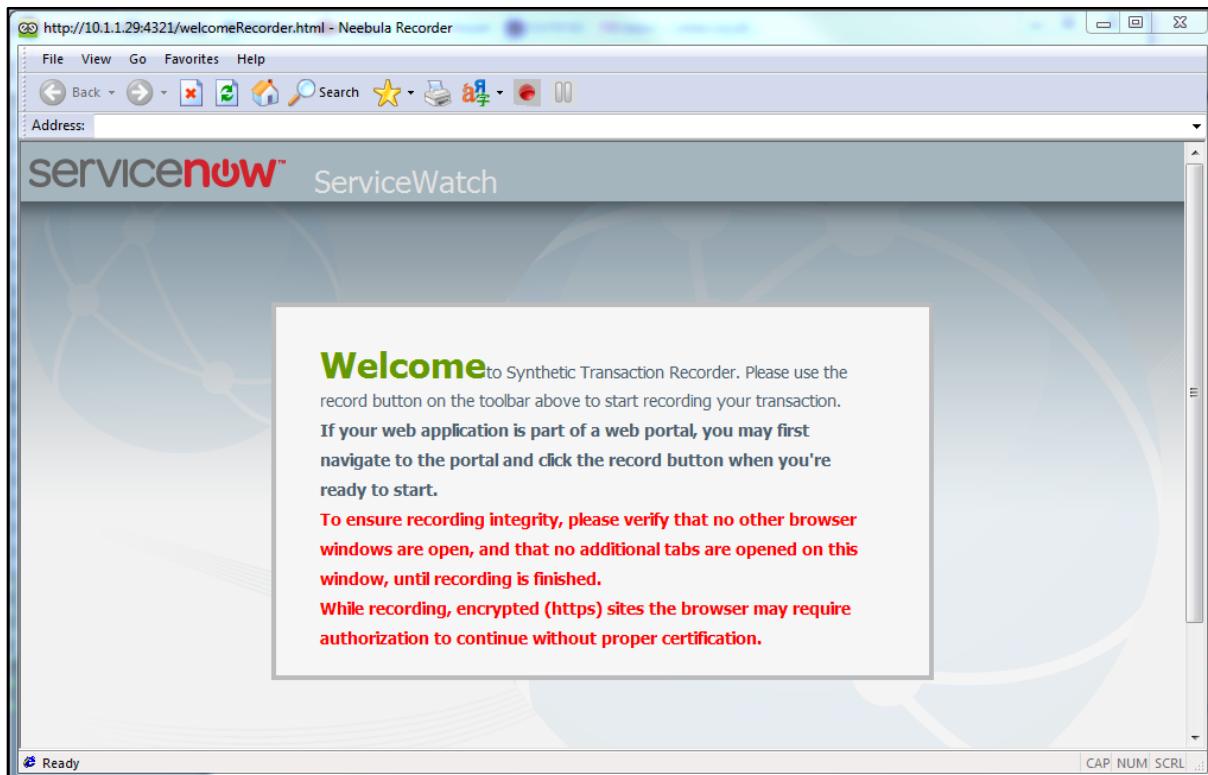
Name	Date modified	Type	Size
Snapshots18672	12/25/2013 5:32 PM	File folder	
MinHook.x86.dll	12/25/2013 5:31 PM	Application extens...	33 KB
params.ini	12/25/2013 5:31 PM	Configuration sett...	1 KB
ServiceWatchRecorder.exe	12/25/2013 5:31 PM	Application	4,299 KB

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

Body contains
Body not contains
Response code equals
Response code not equals

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**



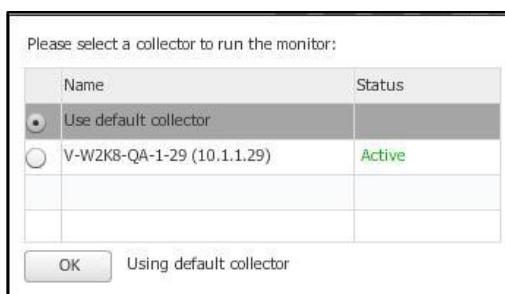
The Search button highlights parameters that contain a specified value. Clicking the button again highlights the next occurrence of that value. After the last occurrence has been displayed, clicking this button will re-display the first occurrence.

**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)

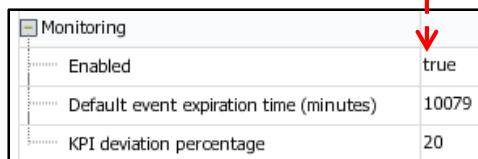
KPIs can be based on *any* integer or floating point number that is meaningful for the user. Obvious examples are CPU usage and percentage of used or unused storage. Less obvious examples are the value of sales or number of customer service tickets per unit of time.

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



Monitoring	
Enabled	true
Default event expiration time (minutes)	10079
KPI deviation percentage	20

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:

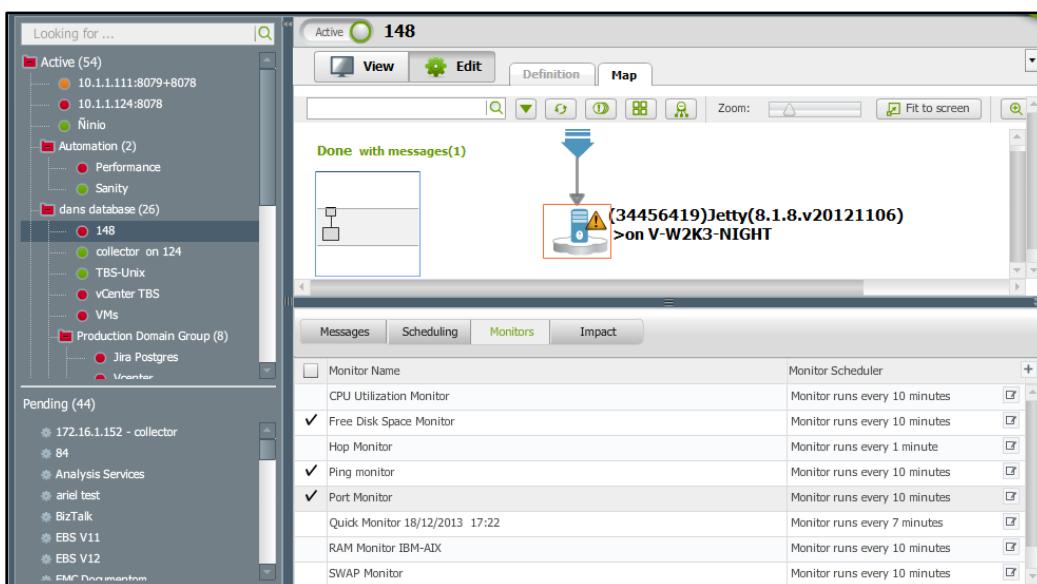
For ascending thresholds, deviation value = value that is dev% below the lowest threshold.

For descending thresholds, deviation value = value that is dev% below the highest threshold.

$KPI = 100 * \text{Abs}(\text{last value} - \text{the deviation value}) / \text{the deviation value}$ .

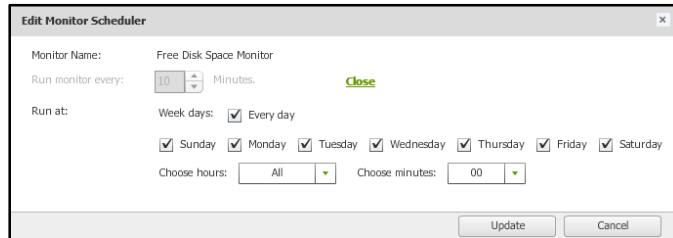
Display the relevant business service topology Map in **Edit** mode. Select the CI whose performance is to be monitored. Click the **Monitors** tab and ensure that the checkboxes for the desired monitors are selected in the **Monitors** panel. You can select the **Monitor Name** checkbox to toggle all 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**

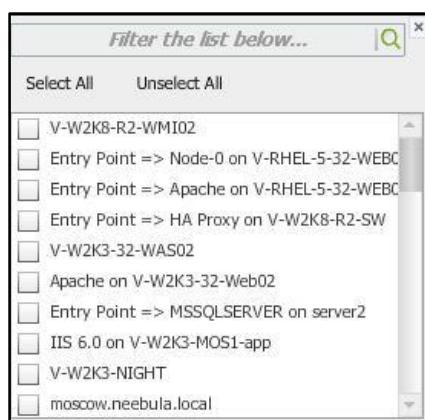
The **Severity** filter prevents the display of monitors whose severity level is less than the position of the filter's slide. Select the slide position, then click the **x** to close the slide and apply the filter.

**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

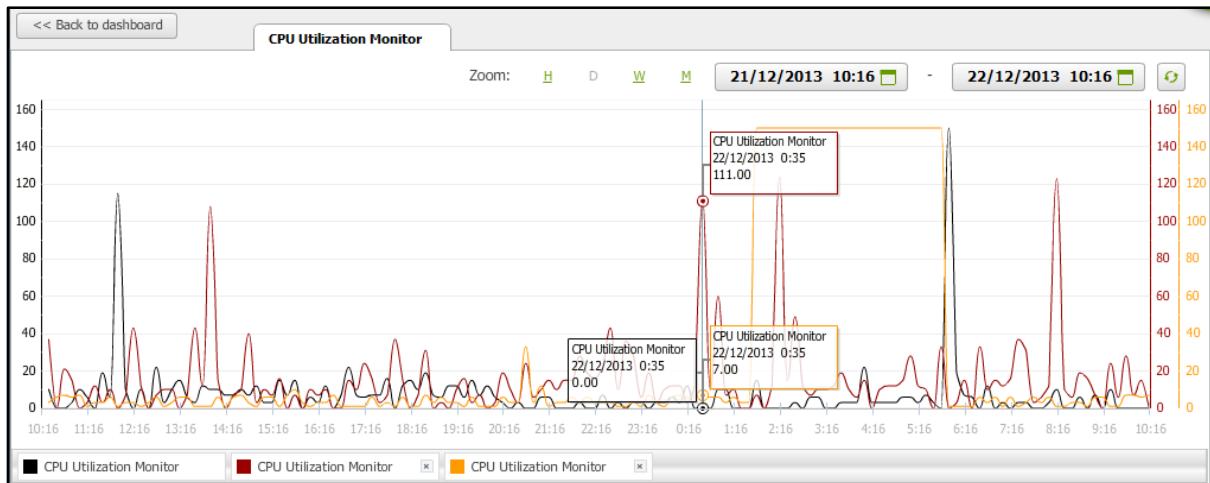


The **H D W M** (Hour, Day, Week, Month) Zoom mechanisms in the upper and lower panels work automatically and independently. Changing either one does not affect the other. However, when using the

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 2<sup>nd</sup>, 3<sup>rd</sup> and/or 4<sup>th</sup> 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  << Back to dashboard in the upper left corner to display the Dashboard.

# Chapter 9: Viewing Business Service History

This chapter contains the following topics:

- Concepts
- Viewing a Business Service's History
- Displaying and Comparing Topology Changes and Details

## 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

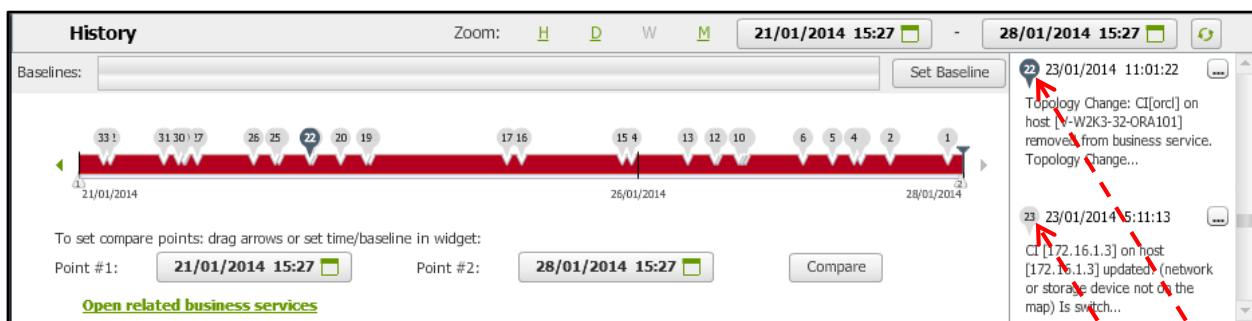
displayed in  mode, the **History** feature enables you to:

- See when changes to the topology of the business service (and related business services) occurred, and to see 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 (22 and 23) 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:

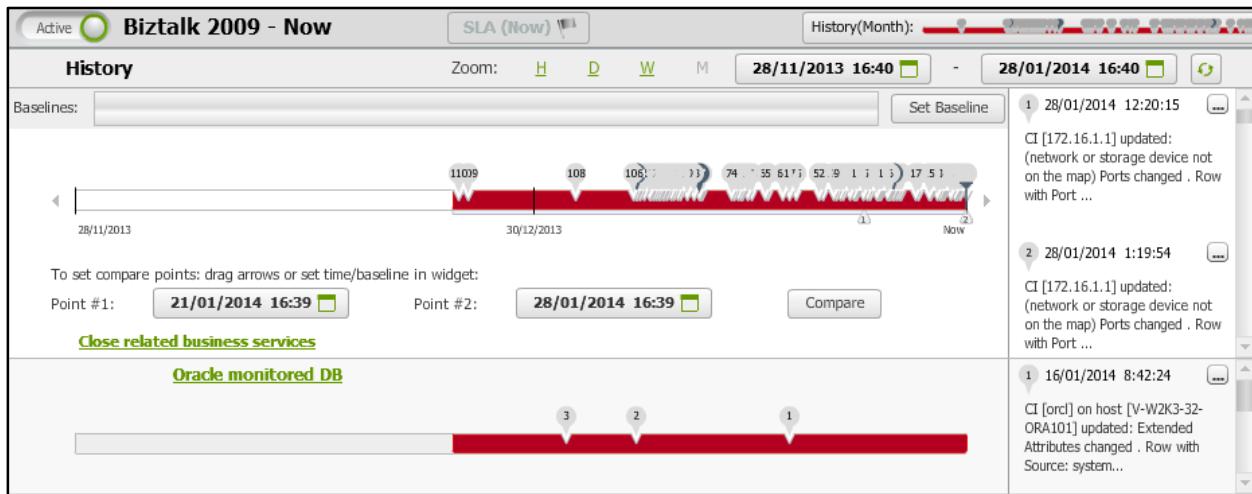
**Table 10: Business Service History actions**

Action	Instructions
To change the scale of the timeline	In the <b>Zoom</b> area above the timeline, click the appropriate time interval ( <b>H</b> = Hour, <b>D</b> = Day, <b>W</b> = Week, <b>M</b> = Month).
To display details of a numbered topology change in a tooltip	Let the cursor hover over the call-out circle, for example  or  Show Now link above the timeline.
To display:	See <a href="#">DISPLAYING AND COMPARING TOPOLOGY CHANGES AND DETAILS</a>
<ul style="list-style-type: none"> <li>▪ timelines for related business services</li> <li>▪ a description of all topology changes</li> <li>▪ the same topology at 2 different times</li> </ul>	
If the arrow at the left  or right  end of the time line is <b>green</b> , 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 **Compare**
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](#)
- [Defining ServiceWatch Network Parameters](#)
- [Displaying Network Path Details](#)
- [Checking the Health of a Network Path](#)

## 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 are usually defined while performing other tasks. Be sure that you have performed the following tasks that involve network parameters:

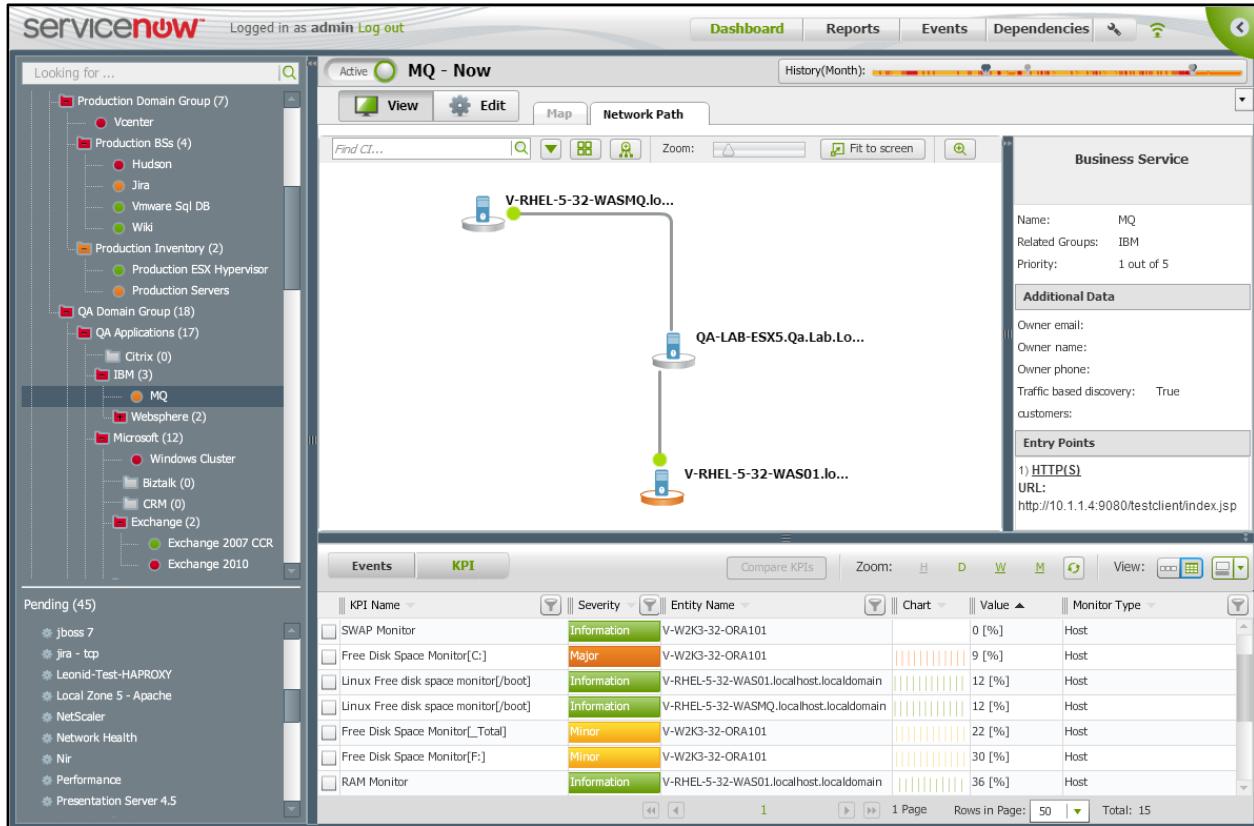
- Defining Network Discovery parameters (see Figure 111 on page 127). This enables ServiceWatch to discover network paths for application flow connections.
- Defining Network Device Impacts and Network impact statuses (see Defining the Impact of an Object on its Parent or Business Service). This enables 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.

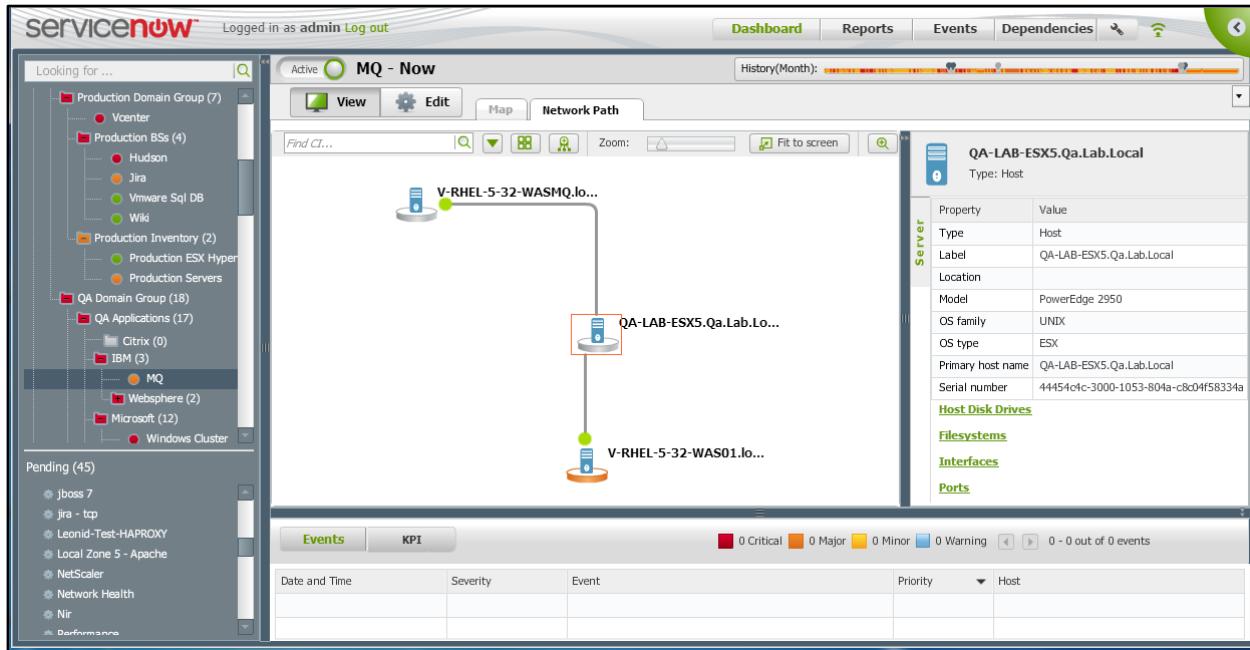
Figure 207: Network Path panel



- ✓ 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 161.

## 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 to exit the pop-up.

**Figure 209: Ports screen – Properties table pop-up**

The pop-up window titled 'Ports on Server' shows a table for the server 'QA-LAB-ESX5.Qa.Lab.Local'. The table has columns for Caption, Description, Hardware Address, Parent Port Identifier, Port Identifier, and State. The table lists various ports, including IDE controllers, PERC, and vmnic interfaces, along with their corresponding hardware addresses and identifiers.

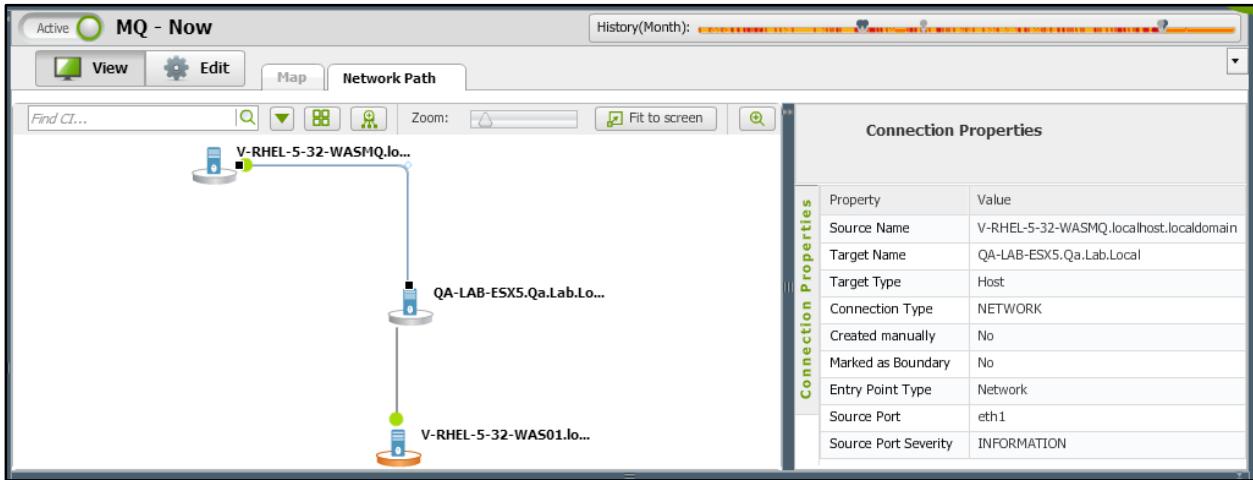
Caption	Description	Hardware Address	Parent Port Identifier	Port Identifier	State
631xESB/632xESB IDE Controller	---	00:1f.1	---	3	---
Dell PERC 6/i Integrated	---	01:00.0	---	2	---
631xESB/632xESB IDE Controller	---	00:1f.1	---	1	---
---	---	00:50:56:67:40:94	---	key-vim.host.VirtualNic-vmk2	---
---	---	00:50:56:6B:A3:97	---	key-vim.host.VirtualNic-vmk1	---
---	---	00:1E:C9:F6:71:C1	---	key-vim.host.VirtualNic-vmk0	---
vmnic3	---	00:15:17:EF:D4:F7	---	vmnic3	---
vmnic2	---	00:15:17:EF:D4:F6	---	vmnic2	---
vmnic1	---	00:1E:C9:F6:71:C3	---	vmnic1	---
vmnic0	---	00:1E:C9:F6:71:C1	---	vmnic0	---

**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](#)

**Business Service**

Name: MQ  
Related Groups: IBM  
Priority: 1 out of 5

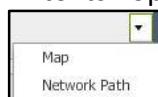
**Additional Data**

Owner email:  
Owner name:  
Owner phone:  
Traffic based discovery: True  
customers:

**Entry Points**

1) HTTP(S)  
URL: http://10.1.1.4:9080/testclient/index.jsp

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**.



near the top right corner and select **Map**.

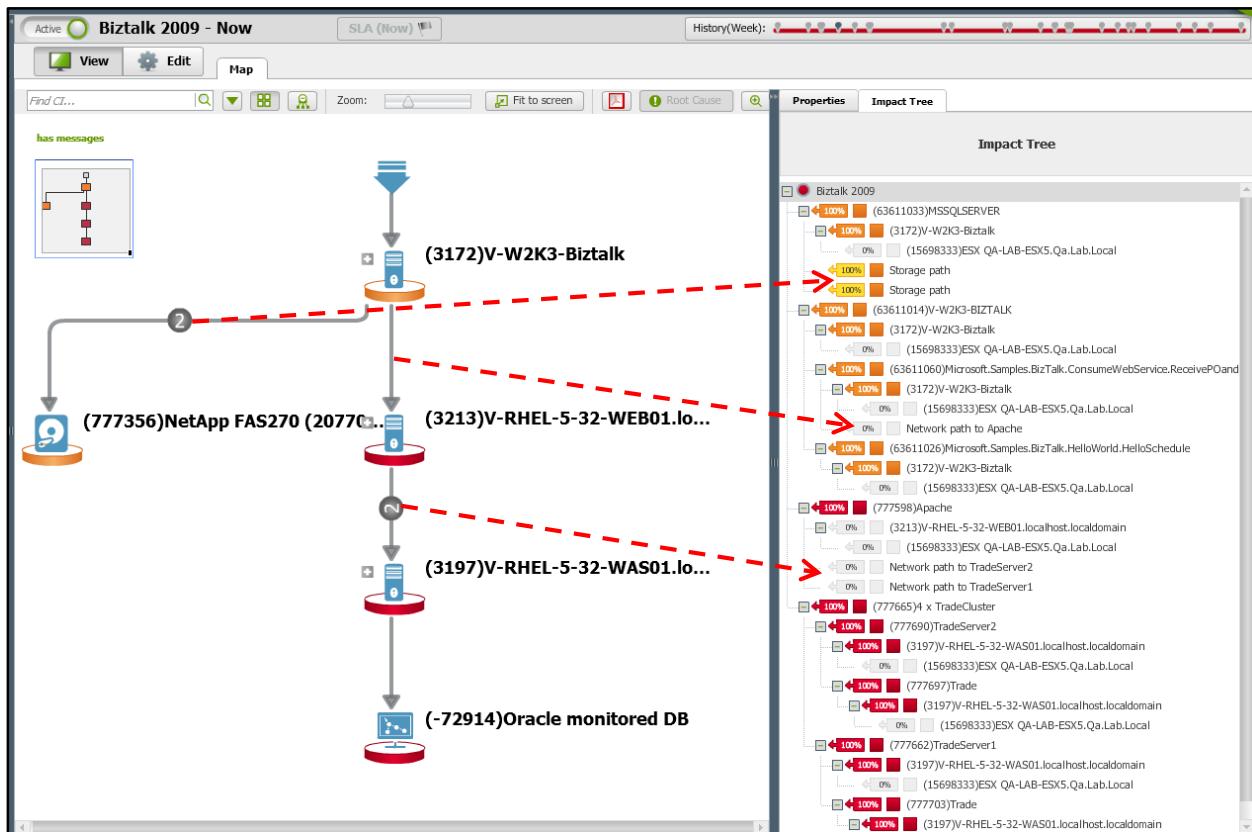
# Checking the Health of a Network Path

As described in Defining the Impact of an Object on its Parent or Business Service on page 142, 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 145).

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.

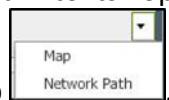
1. Click the business service you want to monitor in the **Active** tree, or double click the tile or bubble of that business service in the Dashboard. When the topology **Map** is displayed, click  and click the **Impact Tree** tab in the pane on the right side. The red dashed lines point to the Storage 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**

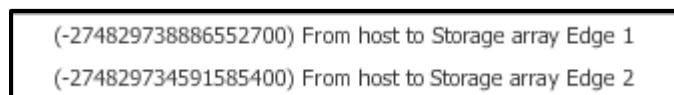


near the top right corner and select **Map**

# Chapter 11: Storage Paths

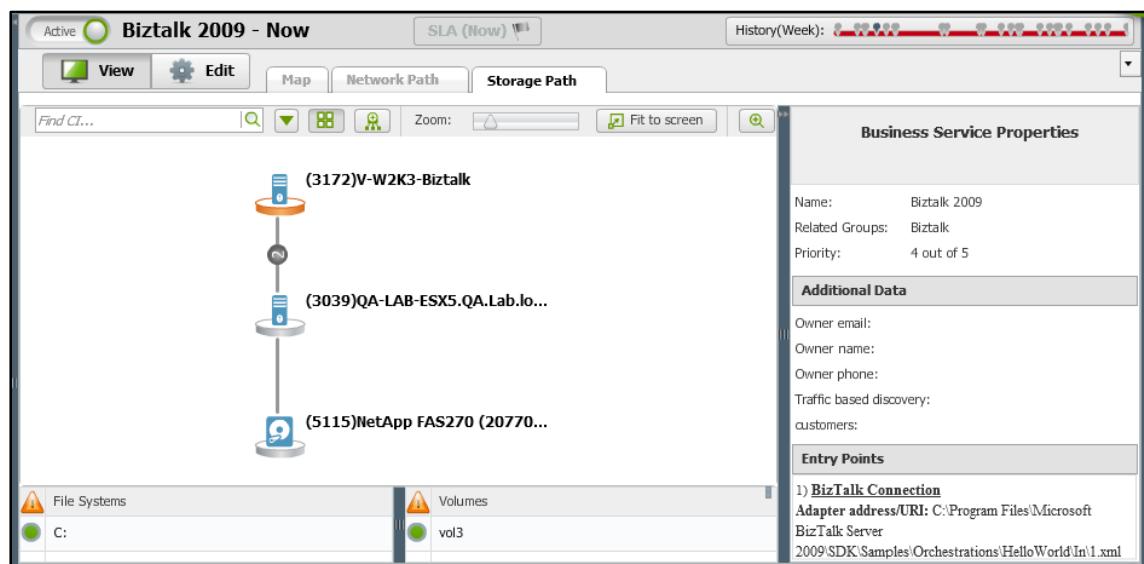
When storage devices are used, it is desirable to monitor the connections between the host and those devices. Storage devices and the paths to them can be discovered using Network Discovery. However, if a storage device for a business service has not yet been discovered, you can specify its IP address 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

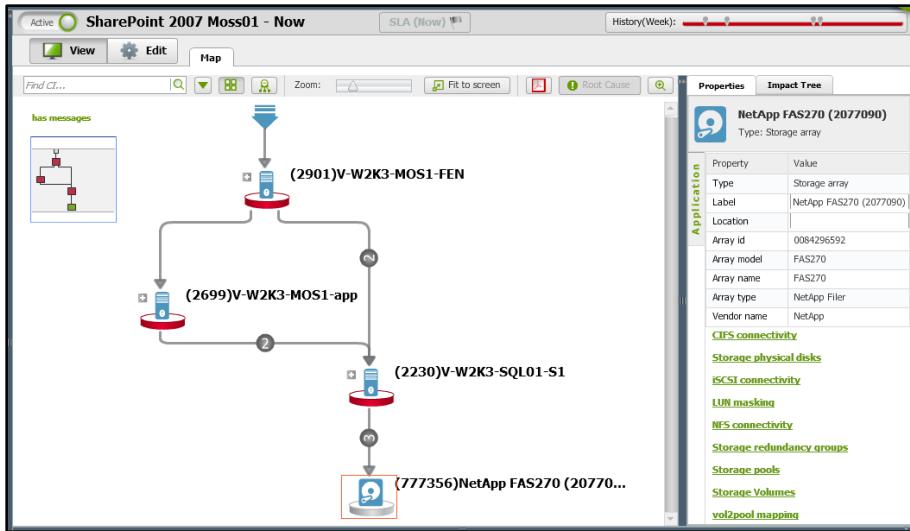
Storage path parameters have defaults, but you can define Network parameters and storage device impact rules when performing the following tasks:

- [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

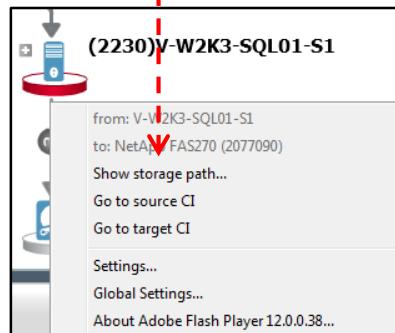
1. Display the topology **Map** for the business service that has a storage device by clicking it in the **Active** tree or double-clicking its tile or bubble in the Dashboard **Monitoring** screen.

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

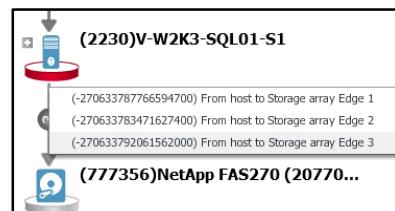
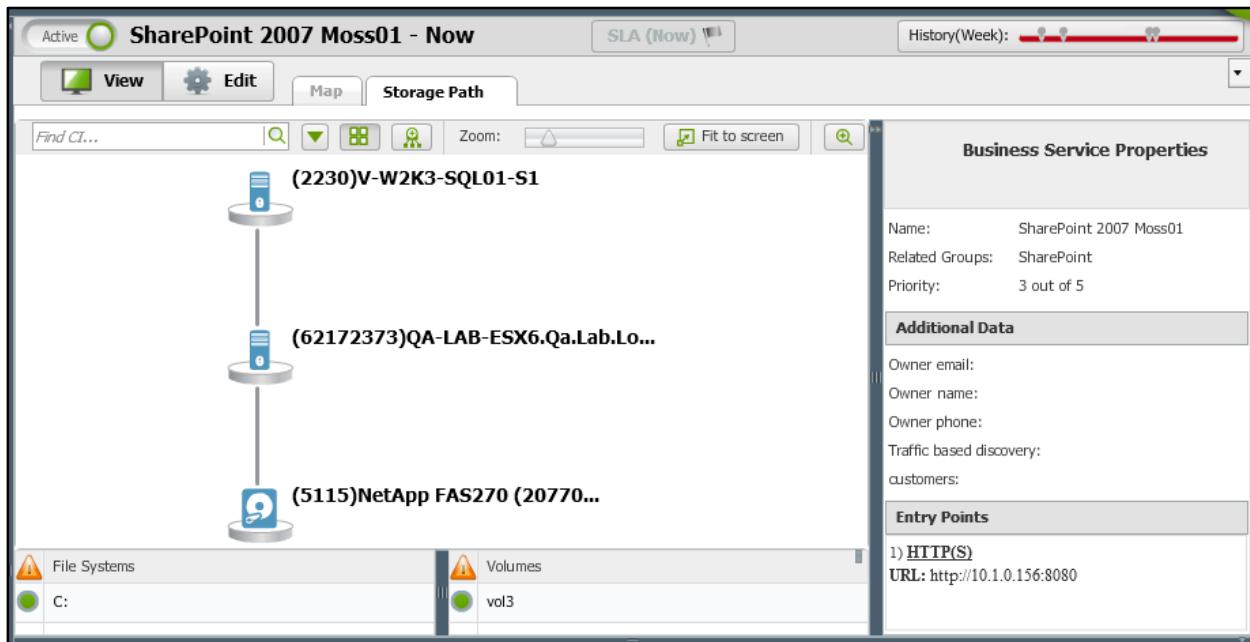


Figure 217: Storage Path panel

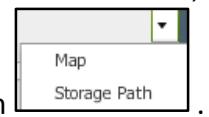


- ✓ Information about the File Systems on the Host and the Volumes on the storage device is displayed in the two panes under the **Storage Path** panel.
  - ✓ Each circle at the end of a connection represents a port or entry point to the storage device.
  - ✓ The Find CI search box, Additional options 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

 <b>NetApp FAS270 (2077090)</b> Type: Storage array <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Property</th> <th style="text-align: left;">Value</th> </tr> </thead> <tbody> <tr> <td>Type</td> <td>Storage array</td> </tr> <tr> <td>Label</td> <td>NetApp FAS270 (2077090)</td> </tr> <tr> <td>Location</td> <td></td> </tr> <tr> <td>Array id</td> <td>0084296592</td> </tr> <tr> <td>Model</td> <td></td> </tr> <tr> <td>Array model</td> <td>FAS270</td> </tr> <tr> <td>Array name</td> <td>FAS270</td> </tr> <tr> <td>OS family</td> <td>PROPRIETARY</td> </tr> <tr> <td>OS name</td> <td>NetApp Release 7.2.3: Thu Jul 5 10:06:16 PDT 2007</td> </tr> <tr> <td>OS type</td> <td>NETAPP</td> </tr> <tr> <td>OS version</td> <td>NetApp Release 7.2.3: Thu Jul 5 10:06:16 PDT 2007</td> </tr> <tr> <td>Primary host name</td> <td>FAS270.Neebula.local</td> </tr> </tbody> </table>	Property	Value	Type	Storage array	Label	NetApp FAS270 (2077090)	Location		Array id	0084296592	Model		Array model	FAS270	Array name	FAS270	OS family	PROPRIETARY	OS name	NetApp Release 7.2.3: Thu Jul 5 10:06:16 PDT 2007	OS type	NETAPP	OS version	NetApp Release 7.2.3: Thu Jul 5 10:06:16 PDT 2007	Primary host name	FAS270.Neebula.local	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Primary management IP</td> <td style="padding: 2px;">172.16.1.10</td> </tr> <tr> <td style="padding: 2px;">Serial number</td> <td style="padding: 2px;">2077090</td> </tr> <tr> <td style="padding: 2px;">Array type</td> <td style="padding: 2px;">NetApp Filer</td> </tr> <tr> <td style="padding: 2px;">Vendor name</td> <td style="padding: 2px;">NetApp</td> </tr> </table> <p><b>CIFS connectivity</b></p> <p><b>Storage physical disks</b></p> <p><b>Interfaces</b></p> <p><b>iSCSI connectivity</b></p> <p><b>LUN masking</b></p> <p><b>NFS connectivity</b></p> <p><b>Ports</b></p> <p><b>Storage redundancy groups</b></p> <p><b>Storage pools</b></p> <p><b>Storage Volumes</b></p> <p><b>vol2pool mapping</b></p>	Primary management IP	172.16.1.10	Serial number	2077090	Array type	NetApp Filer	Vendor name	NetApp
Property	Value																																		
Type	Storage array																																		
Label	NetApp FAS270 (2077090)																																		
Location																																			
Array id	0084296592																																		
Model																																			
Array model	FAS270																																		
Array name	FAS270																																		
OS family	PROPRIETARY																																		
OS name	NetApp Release 7.2.3: Thu Jul 5 10:06:16 PDT 2007																																		
OS type	NETAPP																																		
OS version	NetApp Release 7.2.3: Thu Jul 5 10:06:16 PDT 2007																																		
Primary host name	FAS270.Neebula.local																																		
Primary management IP	172.16.1.10																																		
Serial number	2077090																																		
Array type	NetApp Filer																																		
Vendor name	NetApp																																		

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

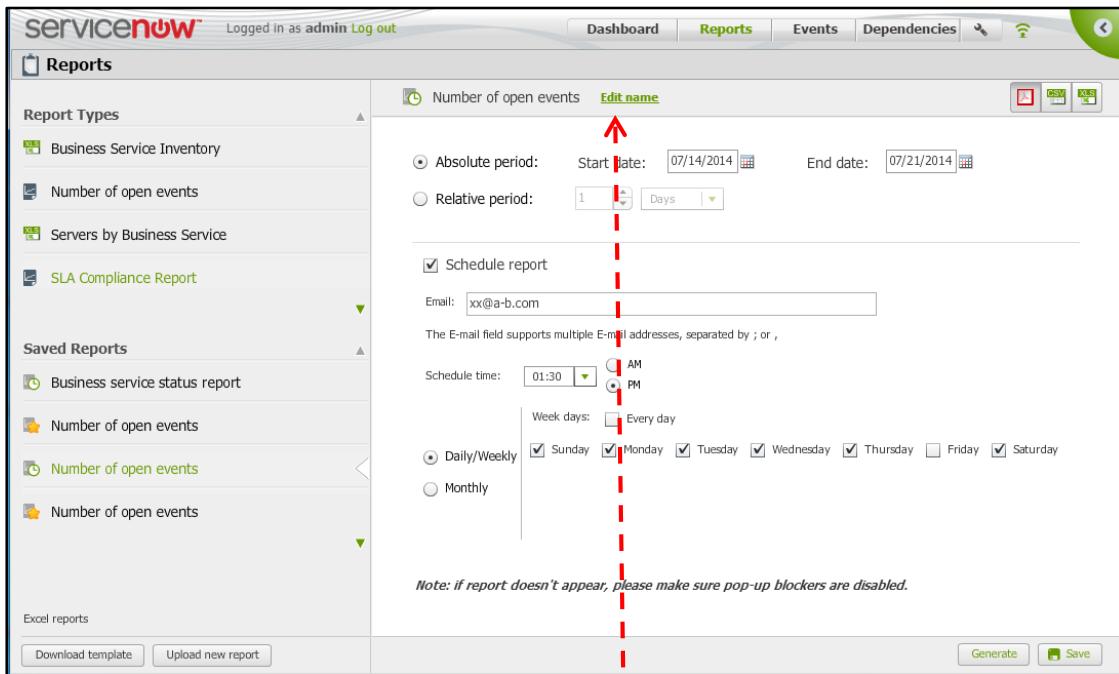
## Report Types

1. The following standard report types are currently available in ServiceWatch:
  - ✓ **Business Service Inventory** – Lists all currently defined Business Services
  - ✓ **Number of open events** for all nodes each day of the report period ([Figure 224](#))
  - ✓ **Servers by Business Service** – Lists all servers and the business services associated with each
  - ✓ **SLA Compliance Report** – Indicates the extent to which Service Level Agreement requirements have been met. See [Figure 225](#) on page [221](#).
  - ✓ **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

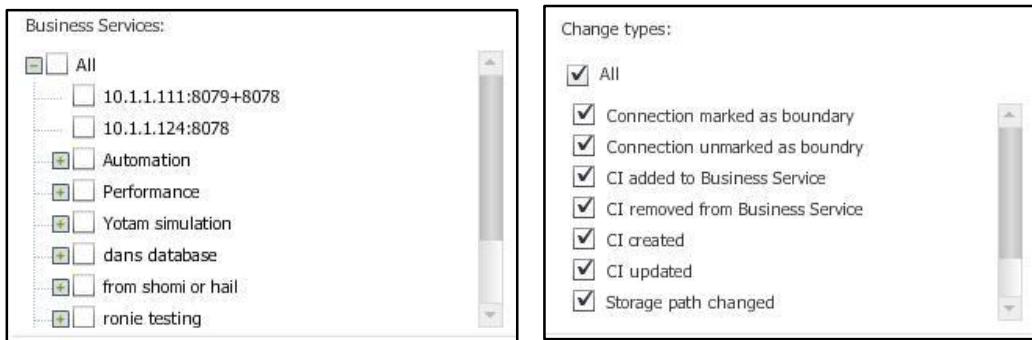
6. Select the **Absolute period** radio button and use calendar icons to specify a **Start & End date**

**Absolute period:** Start date:  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.

**Relative period:**  Days  
Weeks  
Months

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**

This screenshot shows the 'Schedule report' configuration page. It includes fields for 'Email' (with a note about supporting multiple addresses), 'Schedule time' (set to 12:00 AM), and 'Week days' (checkboxes for Every day, Sunday through Saturday). There are also radio buttons for 'Daily/Weekly' and 'Monthly' scheduling.

or the desired months and day of the month

**Figure 222: Schedule report day-of-the-month settings**

This screenshot shows the 'Schedule report' configuration page for monthly scheduling. It includes fields for 'Schedule time' (00:00), 'Months' (checkboxes for Every month, January through December), and 'On day' (a dropdown menu set to 1). A note indicates that 'Of selected months' is available for the 'On day' field.

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. {0.

## Sample Reports

**Figure 224: Number of opened events report**

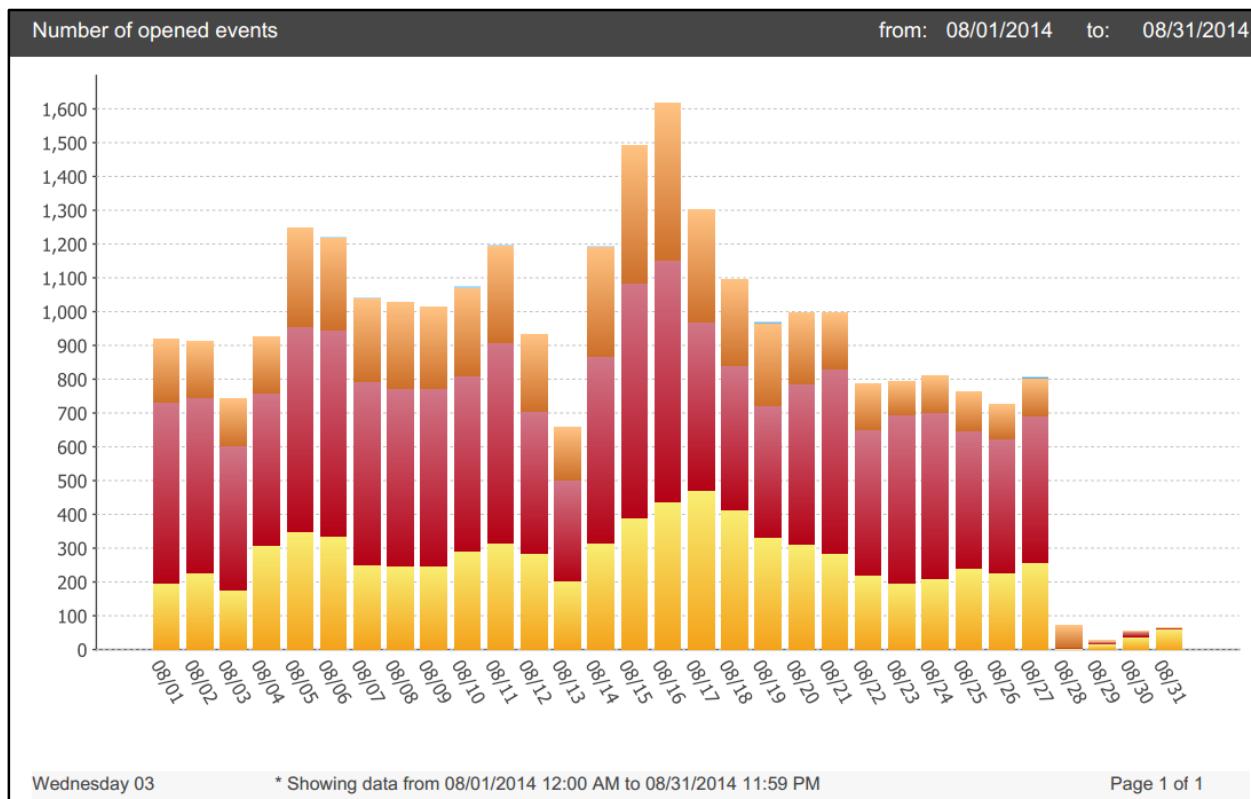
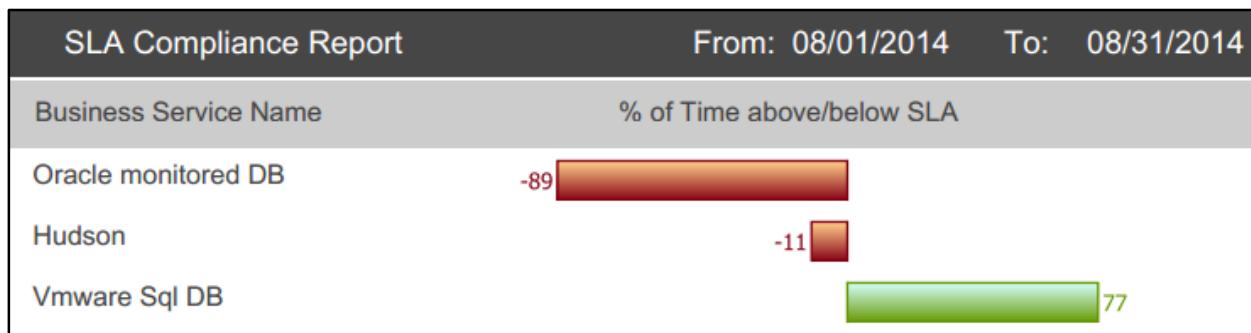


Figure 225: SLA Compliance Report



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  Absolute period:  End date:  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.

Relative period:  Days  
 Schedule report

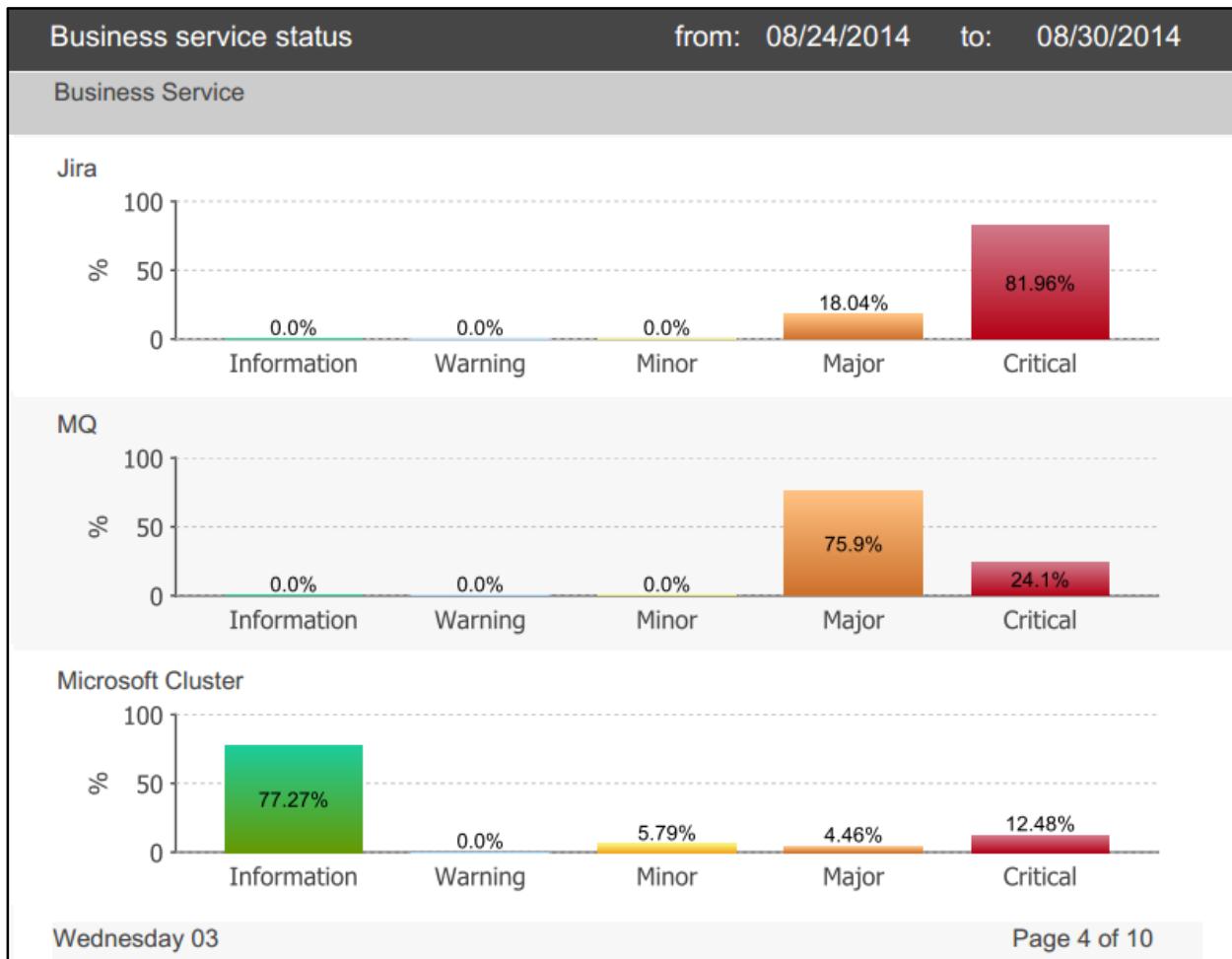
Figure 226: Business service status report



**Figure 227: Topology change report**

Topology change report	
Changes in	from:
apache	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

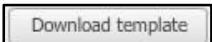
This feature provides an Excel template for designing and generating custom made reports.  
*It requires Microsoft Office 2007 or later.*

**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{0}.

## 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.xlsm	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**.

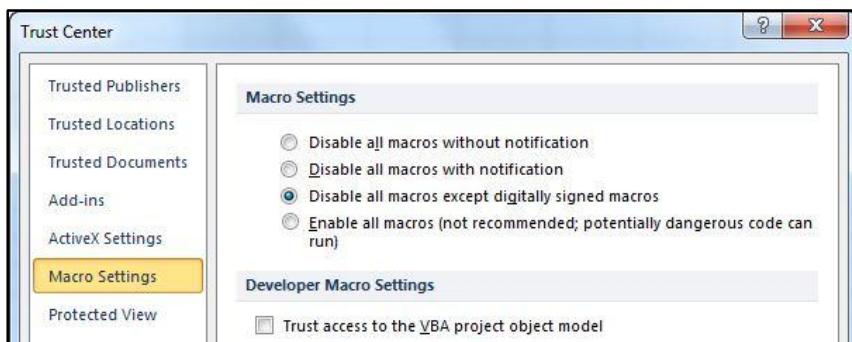
## Method 2

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.

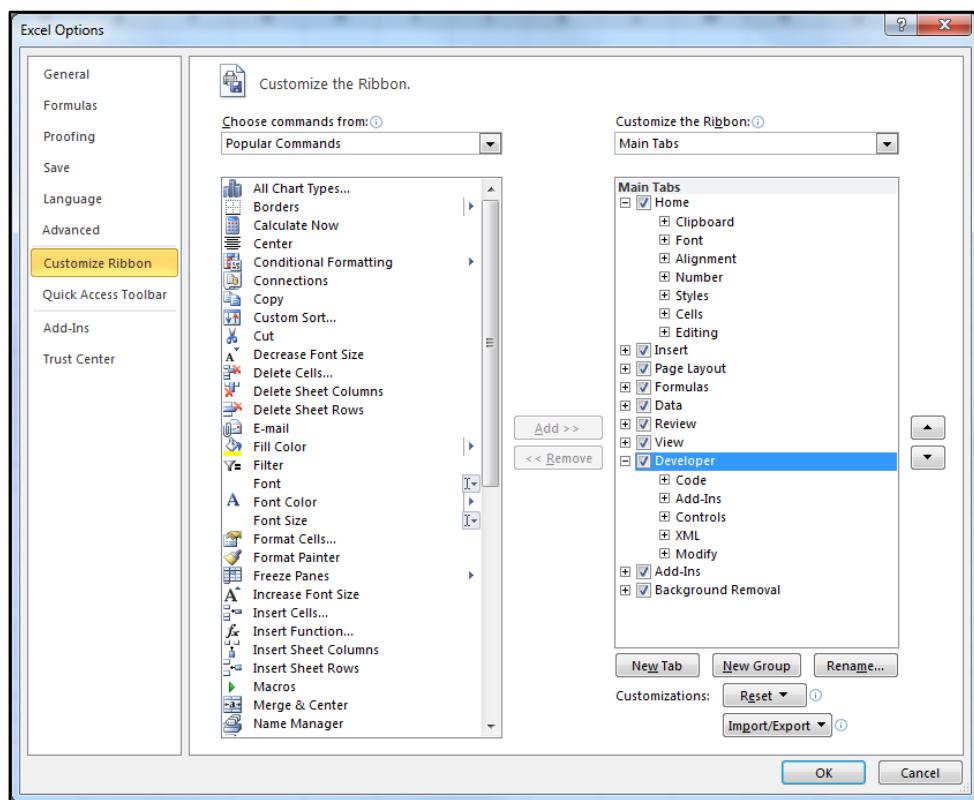


4. Click **Macro Settings** and select the **Enable all macros** radio button.

## 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



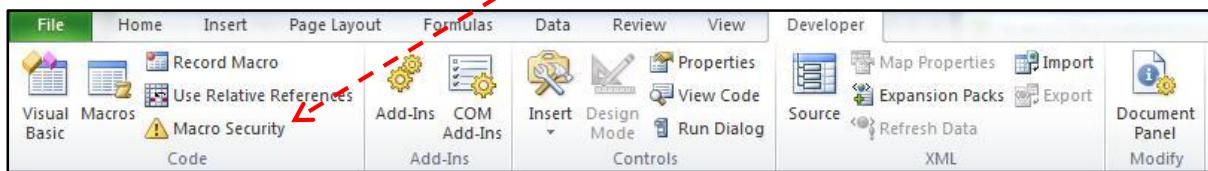
2. Select the **Developer** checkbox in the **Main Tabs** menu, and click **OK**.

The **Developer** tab should appear at the top of the screen.



3. Select the **Developer** tab and its **Macro Security** option.

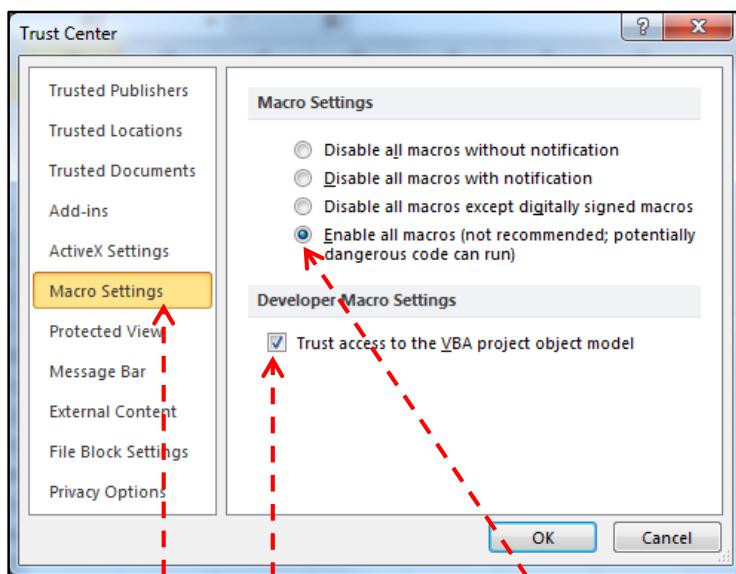
Figure 232: Macro Security option of the Developer panel



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

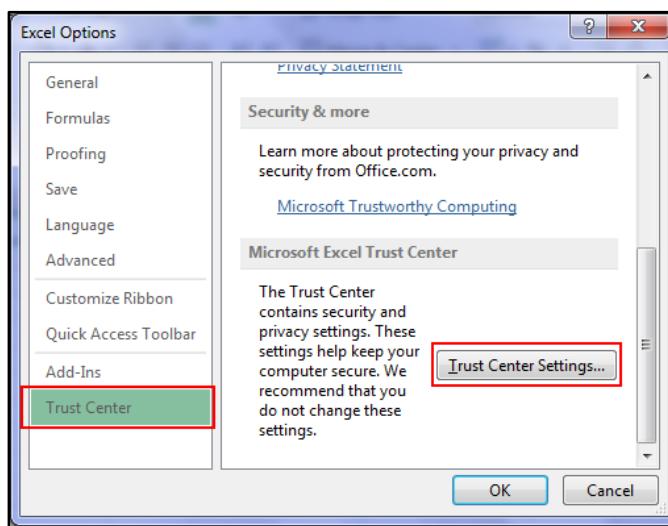


5. In the left panel, select **Macro Settings**, select the **Enable all macros** radio button, and select the **Trust access to the VBA project object model** checkbox.

## 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**.

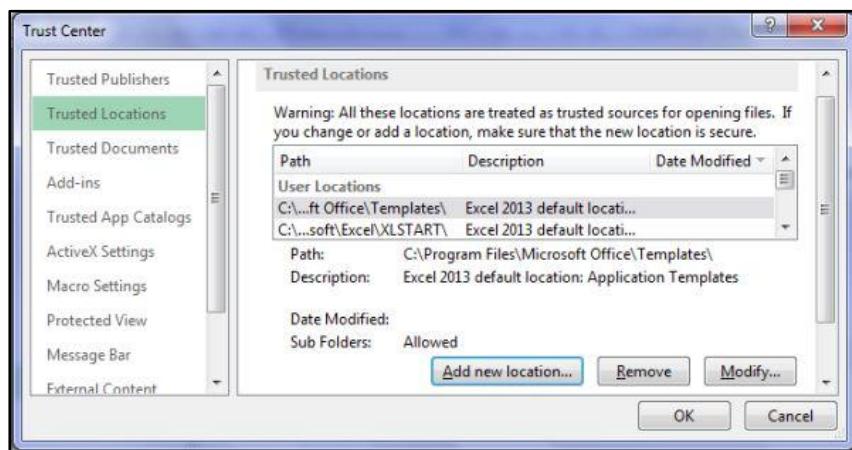
## Method 2

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



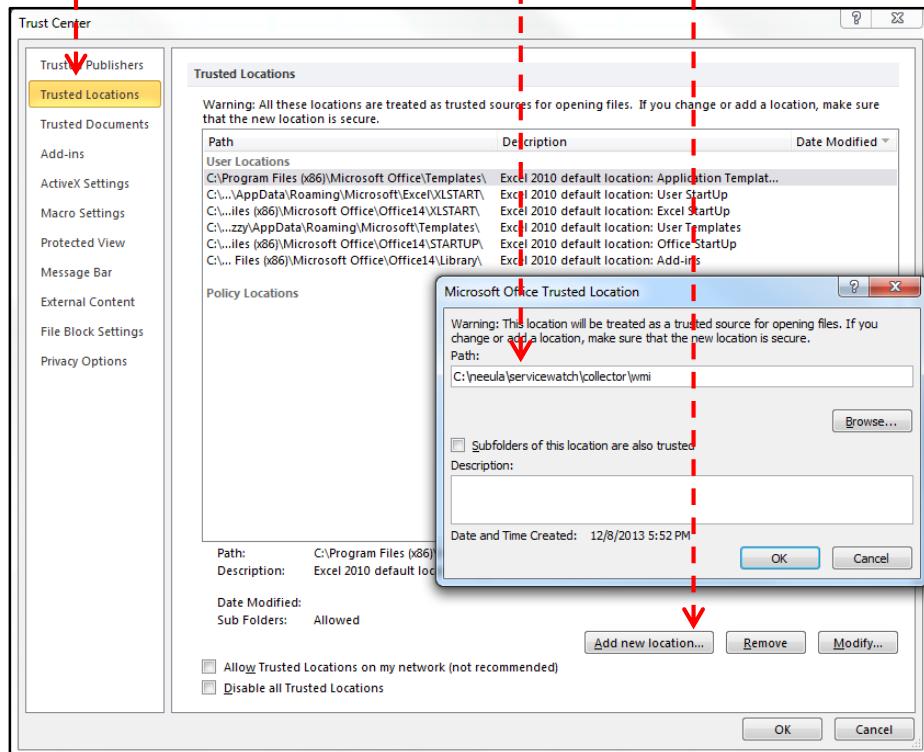
2. Click the **Add new location** button to designate any path as a Trusted Location.

**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

- 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. Click **OK**.

Figure 234: Trusted Locations option of the Trust Center screen



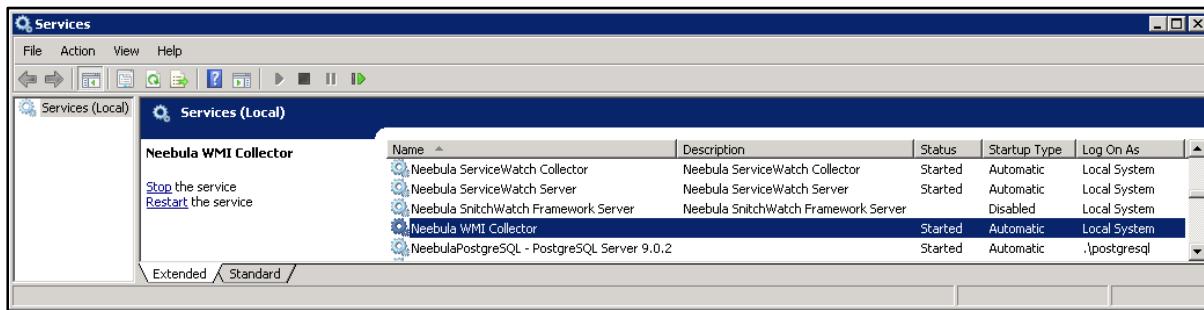
- Confirm that the new location was added, then click **OK** to exit the **Trust Center** window.

Figure 235: Trusted Locations Path list

Path	Description	Date Modified
User Locations C:\neebula\servicewatch\collector\wmi\		12/8/2013 5:52 PM

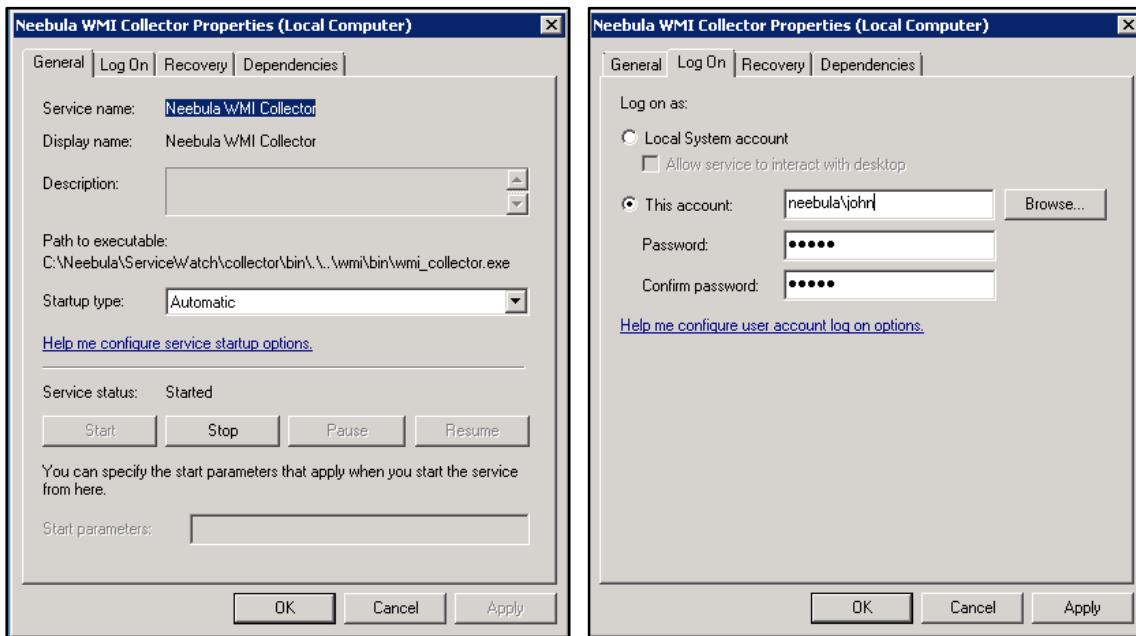
- Open the Windows **Services** screen of the machine on which the on-site WMI Collector runs and scroll to the row that contains **WMI Collector**.

Figure 236: WMI Collector in the Windows Services screen



- 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



- 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.
- 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**.

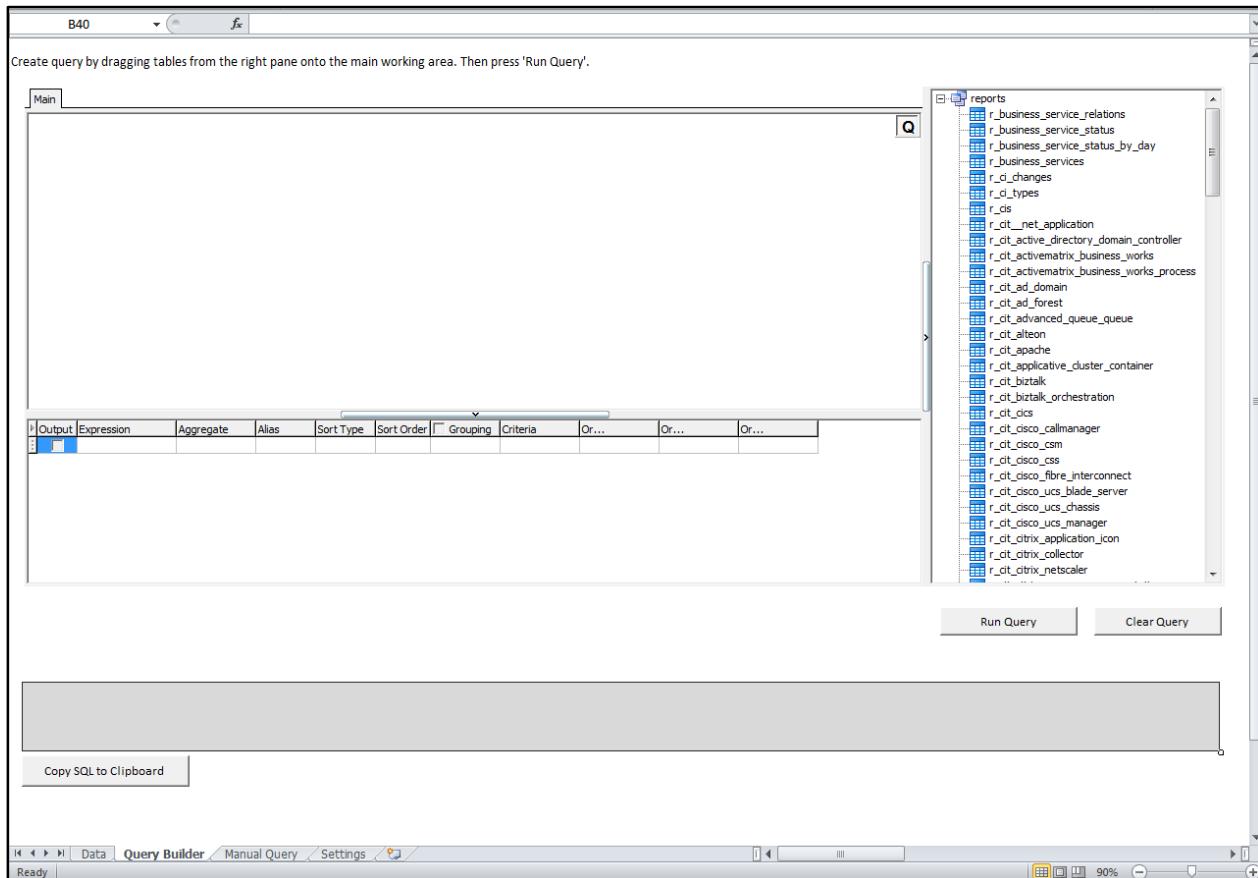
## Using the Excel SQL Query Reports Generator

To design a custom report, run the extracted **ServiceWatch\_customized\_report.xlsx** 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.

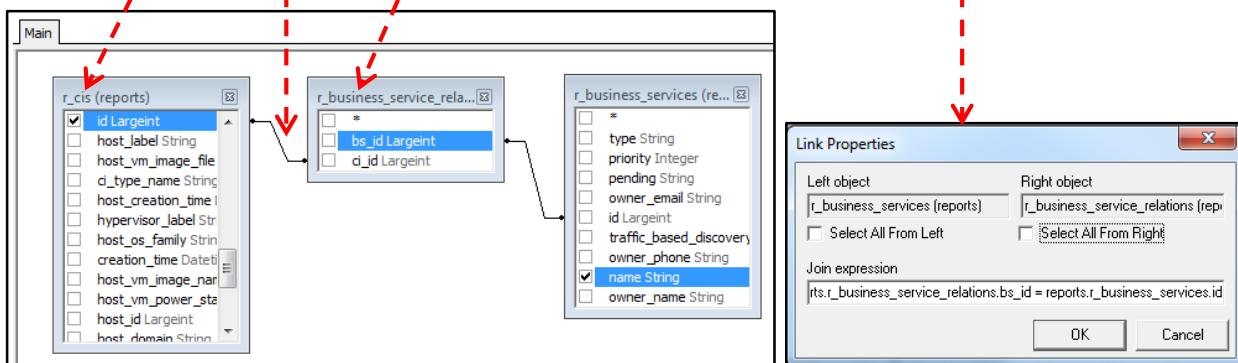
To specify or modify the settings for this application, click the **Settings** tab at the bottom of the screen.

## ***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...
	<input checked="" type="checkbox"/> reports.r_cis.label					<input type="checkbox"/>				
	<input checked="" type="checkbox"/> reports.r_cis.host_os_name					<input type="checkbox"/>				
	<input checked="" type="checkbox"/> reports.r_cis.host_primary_host_name					<input type="checkbox"/>				
	<input checked="" type="checkbox"/> reports.r_business_services.name					<input type="checkbox"/>				
	<input checked="" type="checkbox"/> reports.r_cis.id					<input type="checkbox"/>				
	<input type="checkbox"/>									

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.

	Output	Expression	Aggregate	Alias	Sort Type	Sort Order	Grouping	Criteria for	Criteria	Or...	Or...	Or...
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			Avg Avg Distinct Count Count Distinct Max Max Distinct Min Min Distinct Sum Sum Distinct		Ascending Descending	1		For values For values For groups				

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.

	Output	Expression
1	<input checked="" type="checkbox"/>	reports.r_business_services.name
2	<input checked="" type="checkbox"/>	reports.r_cis.label
3	<input checked="" type="checkbox"/>	reports.r_cis_ci_type_name
4	<input checked="" type="checkbox"/>	reports.r_cis.host_label

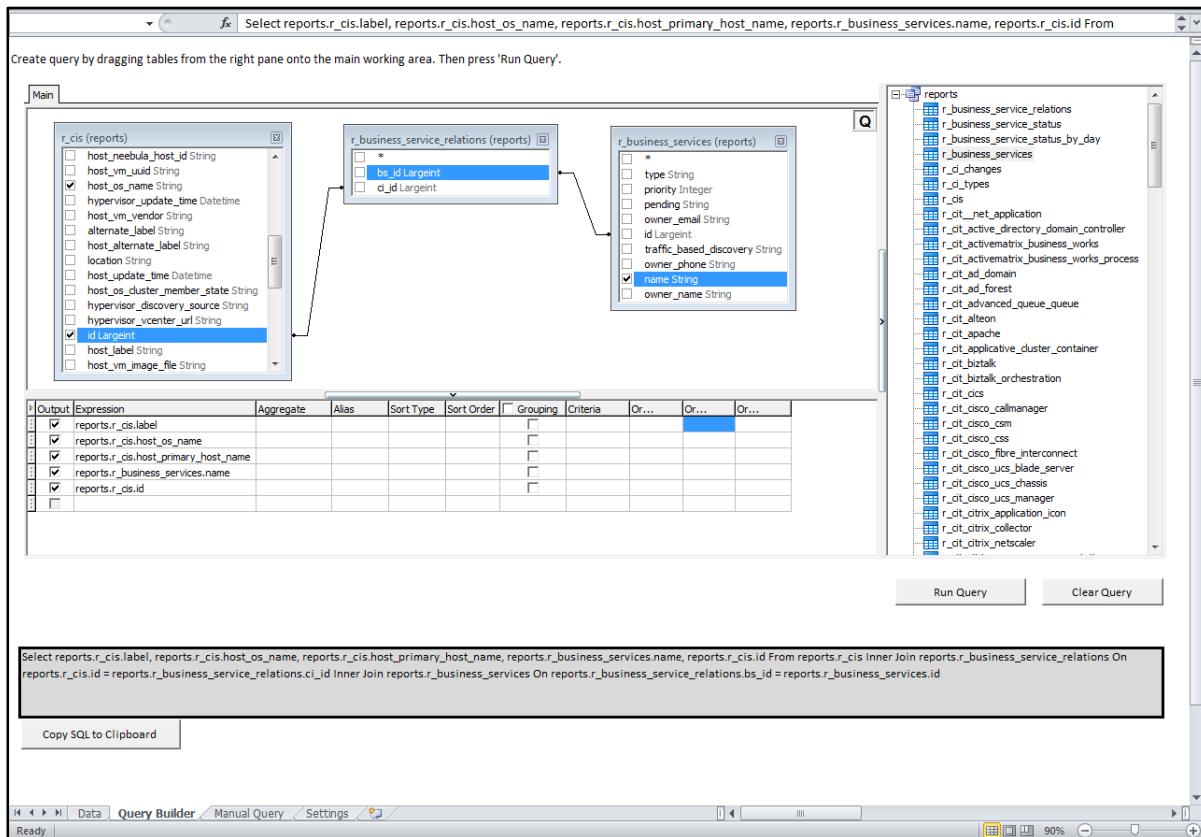
	Output	Expression
1	<input checked="" type="checkbox"/>	reports.r_business_services.name
2	<input checked="" type="checkbox"/>	reports.r_cis.label
3	<input checked="" type="checkbox"/>	reports.r_cis_ci_type_name
4	<input checked="" type="checkbox"/>	reports.r_cis.host_label

The defined SQL statement is automatically displayed and dynamically modified in the grey textbox.

```
Select 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 From reports.r_cis Inner Join reports.r_business_service_relations On reports.r_cis.id = reports.r_business_service_relations.ci_id Inner Join reports.r_business_services On reports.r_business_service_relations.bs_id = reports.r_business_services.id
```

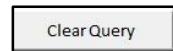
## ***Sample Query built graphically***

**Figure 241: Sample query built graphically**

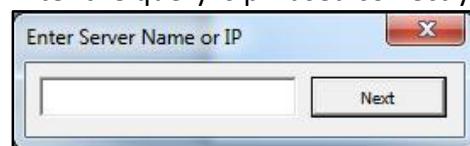


To copy the SQL statement from the textbox to your clipboard, click [Copy SQL to Clipboard](#). One reason for doing this is to paste a graphically-built query into the textbox of the Manual Query tab so that a sophisticated SQL user can make complicated modifications that cannot be implemented by the graphical Query Builder.

To erase the contents of the Query Builder textbox *without* running the query, click



After the query is phrased correctly, click **Run Query**, 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

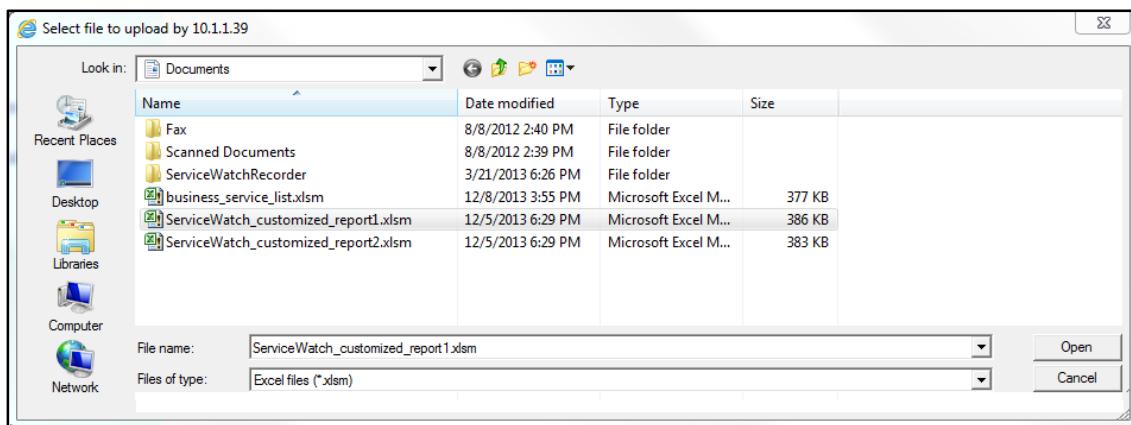
Report Name				
host_os_name	id	host_primary_host_name	name	label
	80		test2	berlin
	80		test1	berlin
	80		test3	berlin
	98		test1	WsusServer
		125	test3	Prod-Esx-15.neebula
		125	test2	Prod-Esx-15.neebula
	142	Prod-Esx-15.neebula	test3	ESX Prod-Esx-15.neebula
	142	Prod-Esx-15.neebula	test2	ESX Prod-Esx-15.neebula

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 **Upload new report** in the bottom left corner of the ServiceWatch Reports screen.

Figure 243: Select file to upload by <IP address> window



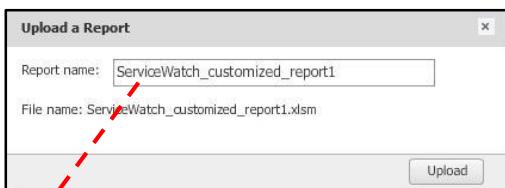
Select the report to upload in the **Select file to upload by <IP address>** window and click

**Open**

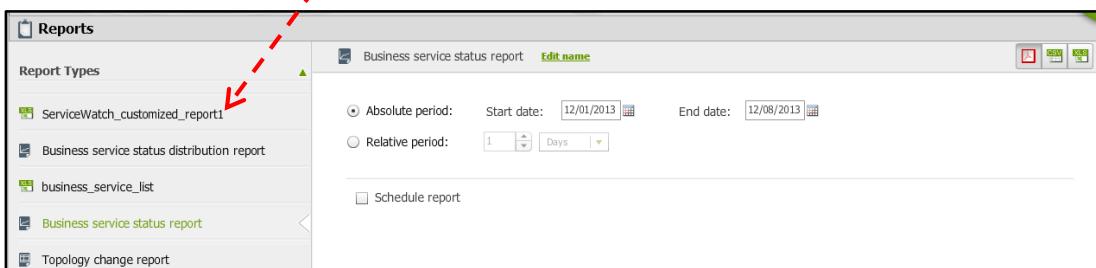
If the Report name in the **Upload a Report** confirmation box is the report you want, click

**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.

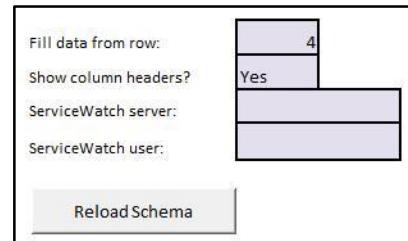
Show column headers? defaults to Yes.

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](http://servicewatch.servicenow.com) in this field.

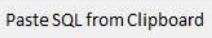
Later, this field defaults to the value you entered.

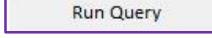
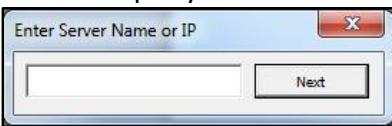
Manually enter the ServiceWatch user name for the first report. Later, it defaults to that value.

After setting or modifying any schema values, click .



## Manual Query tab

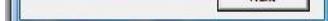
Click the Manual Query tab to display a large grey textbox where you can type in and modify an SQL query. You can also use the  button.

After the query is written correctly, click , type the Server Name or IP in the  dialog box, and click Next.

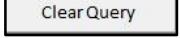
### ServiceWatch Credentials dialog box

Figure 245: ServiceWatch Credentials dialog box



In the , 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 .

# 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.

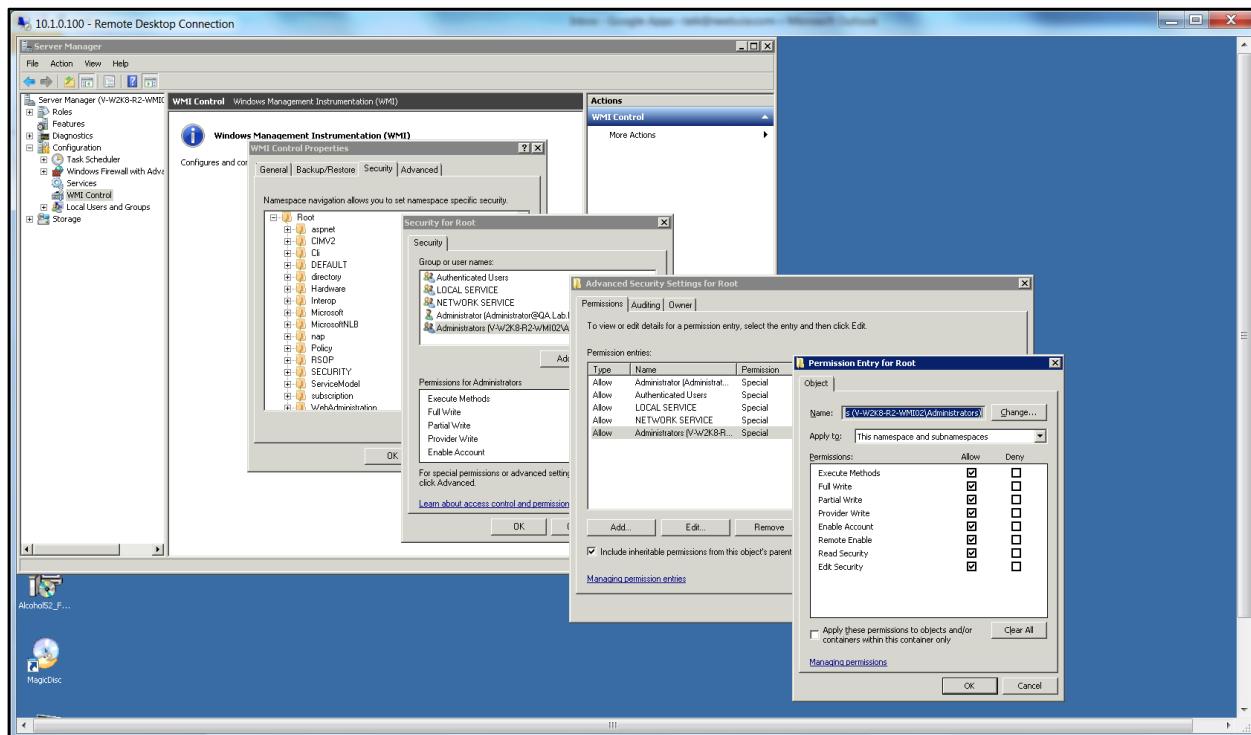
The following services should be running or able to start on demand:

- 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.

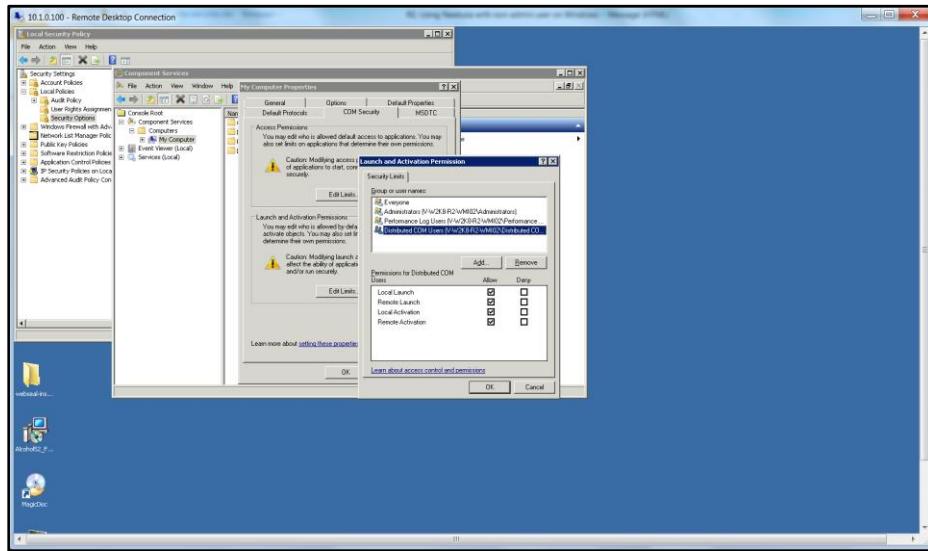
Figure 246: WMI Ctrl > WMI Ctrl Prop. > Security for root > Adv. Security...> Permission Entry...



## 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...](#)



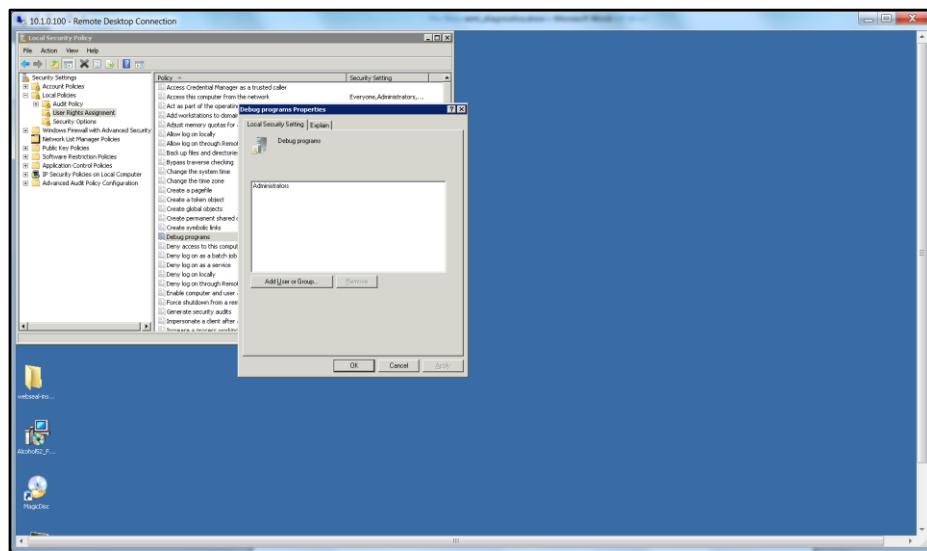
## Verify Security Policy

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

## Chapter 13: Troubleshooting

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
<b>r_business_service_relations</b>	Relation between CIs and business services
Ci_id	CI identifier
Bs_id	Business service identifier
<b>r_business_service_status</b>	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
<b>r_business_service_status_by_day</b>	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

## Appendix B: Schemas for Tables &amp; Views

Table or View / Column Header	Description
Part_of_day	Decimal fraction of the day (from 0.0000 to 1.0000) during which a business service was in that status.
<b>r_business_services</b>	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
<b>r_ci_changes</b>	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
<b>r_ci_types</b>	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)
<b>r_cis</b>	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.

## Appendix B: Schemas for Tables &amp; Views

Table or View / Column Header	Description
<b>r_cit_&lt;name of the CI type&gt;</b> For example: <b>r_cit_apache</b>	The view name starts with <b>r_cit_</b> 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
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
<b>r_connection_types</b>	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
<b>r_connections</b>	<p>Lists all connections in the system. The following connections (which describe relationships between CIs) are listed:</p> <ul style="list-style-type: none"> <li>INCLUSION – a parent (e.g., WebSphere) – child (e.g., WebSphere EAR) relation.</li> <li>APPLICATION_FLOW – a data-flow connection between 2 CIs in a business service</li> <li>CLUSTER – cluster controller (e.g., load balancer) – cluster member connection</li> <li>CLUSTER_MEMBER – an internal CI (an applicative_cluster) – member connection</li> <li>STORAGE_FLOW <ul style="list-style-type: none"> <li>– connections between applications (e.g., PostgreSQL database) – and file systems</li> <li>– connections between a host and fiber channel switches or storage arrays.</li> </ul> </li> <li>NETWORK – connects host – network switch, network switch – switch or router, etc.</li> <li>INTERNAL – internal usage (used by ServiceWatch but not meaningful to a customer)</li> </ul>
Source_ci_id	Source CI identifier
Target_ci_id	Target CI identifier
Connection_category	INCLUSION, APPLICATION_FLOW, CLUSTER, CLUSTER_MEMBER, STORAGE_FLOW, NETWORK, INTERNAL

## Appendix B: Schemas for Tables &amp; Views

Table or View / Column Header	Description
Type	Entry point types in the knowledge base, e.g., HTTP(S), TCP.
<b>r_errors</b>	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
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
<b>r_events</b>	All active and closed events in the system
Id	Event internal identifier
Priority	See <a href="#">Event Priority</a> on page 43
Hostaddress	Address/name of host the event is associated with
Citypname	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

## Appendix B: Schemas for Tables &amp; Views

Table or View / Column Header	Description
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
<b>r_history_changes</b>	Changes detected in a business service over time
Bs_id	Business service ID
Changes	Text description of the change
Time	Time of the change
<b>r_hostnames_ip_addresses</b>	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
<b>r_hosts</b>	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

## Appendix B: Schemas for Tables &amp; Views

Table or View / Column Header	Description
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
<b>r_hypervisors</b>	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
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
<b>r_servers</b>	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

## Appendix B: Schemas for Tables &amp; Views

Table or View / Column Header	Description
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
<b>A</b>	
<b>AD Domain / Forest</b>	<a href="#">Active Directory</a> Domain / Forest
<b>Alteon Load Balancer</b>	<a href="#">Load Balancing</a>
<b>AMAZON_AWS</b>	<a href="#">Amazon Web Services</a>
<b>Apache Web Server</b>	<a href="#">Apache Web Server guide</a>
<b>apikey</b>	<a href="#">Application programming interface key</a>
<b>Application Cluster</b>	Because servers can easily be added or removed from the cluster as needs dictate, an <b>application cluster</b> is more scalable than its hardware-based counterpart. See <a href="#">RAC</a> .
<b>Applicative cluster</b>	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.
<b>Applicative credential type</b>	The Applicative credential type is used for discovering an application or for using an application to discover a connection.
<b>AWS</b>	<a href="#">Amazon Web Services (AWS)</a> is a <a href="#">cloud computing</a> platform offered over the Internet by <a href="#">Amazon.com</a> . Its services include <a href="#">Amazon Elastic Compute Cloud</a> (EC2) and <a href="#">Amazon S3</a> (Simple Storage Service).
<b>B</b>	
<b>bash script</b>	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, <code>sudo bash ./install.sh</code>
<b>BEA Tuxedo</b>	<a href="#">PeopleSoft Application Server</a>
<b>Big-IP GTM</b>	F5 Network <a href="#">Big-IP Global Traffic Manager</a> data sheet
<b>Big-IP LTM</b>	F5 Network <a href="#">Big-IP Local Traffic Manager</a> data sheet
<b>Binding rules</b>	Binding rules connect source fields and values to transformation targets and fields.
<b>BizTalk Orchestration</b>	Represents the underlying logic for processing messages and provides a transactional programming model that supports exception handling and recovery from failed transactions. <a href="#">BizTalk Orchestration</a> .

<b>BizTalk Server</b>	<a href="#">BizTalk Server</a> 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 <a href="#">industry standards like RosettaNet, SWIFT, HL7, HIPAA, etc.</a>
<b>C</b>	
<b>CA</b>	<a href="#">Certificate Authority</a> or Certification Authority that issues <a href="#">digital certificates</a> .
<a href="#">CA eTrust Directory Server</a>	<a href="#">CA Directory overview article</a>
<a href="#">CA Introscope</a>	A component of the CA Application Performance Management solution.
<b>CA Policy Server</b>	CA SiteMinder Policy Server <a href="#">Administration Guide</a> , <a href="#">Configuration Guide</a> , and <a href="#">Installation Guide</a>
<b>CI</b>	Configuration Item
<b>CI type</b>	Type of configuration item, usually indicated on topology maps
<a href="#">CICS</a>	Customer Information Control System is a <a href="#">transaction server</a> that runs on <a href="#">IBM mainframes</a> under <a href="#">z/OS</a> and <a href="#">z/VSE</a> . CICS is <a href="#">middleware</a> that supports rapid, high-volume <a href="#">online transaction processing</a> .
<b>CICS Transaction Gateway</b>	Provides access from Java Client applications to CICS applications, using standard Internet protocols. <a href="#">CICS Transaction Gateway</a>
<a href="#">Cisco CallManager</a>	<a href="#">Cisco CallManager Basic Concepts</a>
<a href="#">Cisco CSM</a>	<a href="#">Cisco Security Manager</a>
<a href="#">Cisco CSS</a>	<a href="#">Cisco Content Services Switch</a>
<a href="#">Cisco Fabric Interconnect</a>	<a href="#">Configuring the Fabric Interconnects</a>
<a href="#">Citrix NetScaler</a>	<a href="#">Citrix NetScaler Cloud Network Platform</a>
<a href="#">Citrix XenApp</a>	See XenApp or Presentation Server EP, an on-demand application delivery solution that allows apps to be virtualized, centralized and managed.
<b>CLI</b>	<a href="#">Command Line Interface</a>
<b>CLI Event Sender</b>	When triggered by an alert, this executable sends an event to the ServiceWatch server.
<b>cmdb</b>	<a href="#">Configuration Management Database</a>
<b>Collector</b>	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.
<b>Connect-It Service</b>	<a href="#">Version 3.70 User's Guide</a> . <a href="#">Version 4.10 User's Guide</a> .
<b>Control-M Enterprise Manager/Gateway/Server</b>	<a href="#">Wikipedia article</a> . <a href="#">Enterprise Manager</a> . <a href="#">Server Administrator Guide</a> .

<b>CSR</b>	<a href="#">Certificate Signing Request</a>
<b>curl program</b>	<b>curl</b> 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 <a href="http://curl.haxx.se/docs/manpage.html">http://curl.haxx.se/docs/manpage.html</a>
<b>D</b>	
<b>DataPower</b>	Self-balancing and intelligent load distribution for application servers. For example, <a href="#">IBM WebSphere DataPower SOA Appliances</a> . See DPT.
<b>DB2 Database Server</b>	<a href="#">IBM DB2</a>
<b>DB2 UDB</b>	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.
<b>DCOM</b>	<a href="#">Distributed Component Object Model</a> is a <a href="#">proprietary Microsoft</a> technology for communication among <a href="#">software components</a> across networked <a href="#">computers</a> . DCOM, which originally was called "Network <a href="#">OLE</a> ", extends <a href="#">Microsoft's COM</a> and provides the communication substrate under <a href="#">Microsoft's COM+</a> application server infrastructure.
<b>Debian GNU/Linux</b>	<a href="#">Debian</a> is a <a href="#">free</a> operating system that uses the <a href="#">Linux</a> kernel but most of the OS tools come from the <a href="#">GNU project</a> ; hence the name GNU/Linux.
<b>DMZ</b>	A <b>Demilitarized Zone</b> is a physical or logical <a href="#">subnetwork</a> 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 <a href="#">local area network</a> . An external attacker can only access objects in the DMZ and cannot access any other part of the network.
<b>Documentum</b>	<a href="#">Brava! Enterprise Webtop Server/Job Processor ver. 6.5</a> <a href="#">Brava Enterprise ver. 7.0 Architecture</a> <a href="#">Content Server Administration and Configuration Guide</a>
<b>Domain Controller</b>	<a href="#">Domain controllers</a> in your network store user account information, authenticate users, and enforce security policy for a Windows domain.
<b>DPT</b>	<a href="#">Data Power Technology</a> . Email: <a href="mailto:info@datapowertech.com">info@datapowertech.com</a>
<b>E</b>	
<b>ECC</b>	EMC Control Center, an application for a storage device from EMC.
<b>EJB</b>	<a href="#">Enterprise JavaBeans</a>

<b>EMC</b>	<a href="#">EMC<sup>2</sup></a>
<b>EMS</b>	Enterprise Message Service, a <a href="#">Java Message Service</a> by <a href="#">Tibco Software</a> <a href="#">Event Monitoring System</a>
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	<a href="#">Enterprise Service Bus</a>
escalationFlag	Values: NORMAL, ESCALATED, ESCALATED_LEVEL2, ESCALATED_LEVEL3, SUPPRESSED
<a href="#">ESX</a>	VMware ESX and ESXi are VMware's <a href="#">enterprise software</a> Type 1 <a href="#">hypervisors</a> for guest virtual servers; they run on <a href="#">hostserver</a> hardware without an underlying <a href="#">operating system</a> .
expireTime	Expiration time
<b>F</b>	
<b>Fast Index Server</b>	<a href="#">Documentum Full Text Index Server</a>
<b>FTP(S)</b>	<a href="#">File Transfer Protocol</a> [with support for <a href="#">Transport Layer Security</a> (TLS) and <a href="#">Secure Sockets Layer</a> (SSL) cryptographic protocols]
<b>G</b>	
<b>Generic Application</b>	Microsoft <a href="#">Generic Application</a>
<b>GNU wget</b>	See wget in this glossary.
<b>GROUNDWORK</b>	<a href="#">GroundWork</a> provides an open software platform for easy integration and customized visualization of cloud, virtualization, network, application, server, and storage data.
<b>H</b>	
<b>HIPAA</b>	<a href="#">Health Insurance Portability and Accountability Act</a>
<a href="#">Hitachi Data Systems</a>	See also <a href="#">Hitachi Storage systems</a>
<b>HL7</b>	<a href="#">Health Level 7</a>
<b>hostAddress</b>	Hostname or IP where a CI (to which an event should be bound) runs.

<a href="#"><b>HP BTO</b></a>	IT management software, aka <a href="#">Business Technology Optimization</a> (BTO) software, is the largest category of software sold by HP.
<a href="#"><b>HP EVA</b></a>	See the <a href="#">HP EVA P6000 Storage data sheet</a>
<a href="#"><b>HP OpenView</b></a>	In 2007, HP OpenView was rebranded as HP BTO (Business Technology Optimization) Software.
<a href="#"><b>HP Operations Manager</b></a>	A <a href="#">software agent</a> 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, <a href="#">trouble-ticket systems</a> , and <a href="#">notification systems</a> .
<a href="#"><b>HP Quality Center</b></a>	<a href="#">HP Quality Center</a> is quality management software from Hewlett-Packard with capabilities acquired from <a href="#">Mercury Interactive</a> Corp. HP Quality Center provides <a href="#">requirements &amp; test management</a> and <a href="#">business process</a> testing for IT and application environments.
<a href="#"><b>HP SM Index Server</b></a>	<a href="#">HP Service Manager</a>
<a href="#"><b>HP uCMDB</b></a>	See <a href="#">Make Your HP uCMDB Service Aware</a> and its <a href="#">Wikipedia</a> article.
<a href="#"><b>HPOM</b></a>	<a href="#">HP Operations Manager</a>
<a href="#"><b>http</b></a>	Hypertext Transfer Protocol. See <a href="http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol">http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol</a>
<a href="#"><b>HTTP Listener to WMB Dependency</b></a>	<a href="#">HTTP Listener to WebSphere Message Broker</a>
<a href="#"><b>HTTPS</b></a>	<a href="#">HTTP Secure protocol</a>
<a href="#"><b>hypervisor</b></a>	A <a href="#">hypervisor</a> or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs <a href="#">virtual machines</a> .
<b>I</b>	
<a href="#"><b>IBM CICS</b></a>	See CICS.
<a href="#"><b>IBM Tivoli Netcool</b></a>	See <a href="#">Netcool</a>
<a href="#"><b>IBM WebSphere Message Broker</b></a>	<a href="#">Lightweight, advanced ESB</a> that integrates data sources from a wide range of platforms across SOA and non-SOA environments.
<a href="#"><b>IBM WebSphere MQ Queue</b></a>	<a href="#">WebSphere Message Queue</a>
<a href="#"><b>IBM WMB Http Listener</b></a>	<a href="#">WebSphere Message Broker http listener</a> (see HTTP Listener)
<a href="#"><b>IIFP Entry Point</b></a>	<a href="#">Identity Integration Feature Pack</a>

<b>IIS Website</b>	<a href="#">Internet Information Services</a>
<b>IMAP</b>	<a href="#">Internet Message Access Protocol</a>
<b>Inetinfo</b>	User-mode component that hosts the IIS metabase and the non-Web services of IIS.
<b>iPlanet</b>	A product brand used jointly by <a href="#">Sun Microsystems</a> and <a href="#">Netscape Communications Corporation</a> when delivering software and services as part of a non-exclusive cross marketing deal.
<b>ISA Server</b>	<a href="#">ISA Server</a> and <a href="http://www.isaserver.org/">http://www.isaserver.org/</a>
<b>ISAM</b>	<i>Indexed Sequential Access Method</i> , a method for <a href="#">indexing</a> data for fast retrieval. Originally developed by <a href="#">IBM</a> for <a href="#">mainframe computers</a> .
<b>J</b>	
<b>Java KeyStore</b>	A <a href="#">Java KeyStore</a> (JKS) is a repository of security certificates, either <a href="#">authorization certificates</a> or <a href="#">public key certificates</a> , used in <a href="#">SSL encryption</a> .
<b>JAXB</b>	<a href="#">Java Architecture for XML Binding</a>
<b>JBoss AS</b>	<a href="#">JBoss Application Server</a> . JBoss is a division of Red Hat.
<b>JDBC</b>	<a href="#">Java Database Connectivity</a> 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.
<b>Jetty</b>	<a href="#">Jetty</a> is a pure <a href="#">Java</a> -based <a href="#">HTTP (Web) server</a> and <a href="#">Java Servlet</a> container.
<b>JIRA</b>	Project and issue tracking software by Atlassian
<b>JMS</b>	<a href="#">Java Message Service</a> <a href="http://en.wikipedia.org/wiki/Java_Message_Service">http://en.wikipedia.org/wiki/Java_Message_Service</a>
<b>Jrun WAR</b>	<a href="#">JRun</a> 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.
<b>JSSE</b>	<a href="#">Java Secure Socket Extension</a> provides a set of packages which enable secure <a href="#">Internet</a> communications. It implements a <a href="#">Java</a> version of the <a href="#">Secure Sockets Layer</a> (SSL) and <a href="#">Transport Layer Security</a> (TLS) <a href="#">protocols</a> . It includes functionality for data <a href="#">encryption</a> , server <a href="#">authentication</a> , <a href="#">message integrity</a> , and optional client-authentication.
<b>K</b>	

<b>Kerberos</b>	<a href="#">Kerberos</a> is a <a href="#">computer network authentication protocol</a> that uses "tickets" to allow <a href="#">nodes</a> communicating over a non-secure network to prove their identity to one another in a secure manner.
<a href="#"><b>KeyStore</b></a>	A <b>Java KeyStore</b> is a repository of security certificates used for instance in <a href="#">SSL encryption</a> . In <a href="#">Oracle WebLogic Server</a> , a file with extension <code>jks</code> is the keystore. The <a href="#">Java Development Kit</a> maintains a <a href="#">CA</a> keystore in folder <code>jre/lib/security/cacerts</code> . JDKs provide a tool named <code>keytool</code> to manipulate the keystore. <code>keytool</code> cannot extract the private key out of the keystore, but this is possible with 3rd-party tools like <code>JKSExportKey</code> , <a href="#">CERTIVITY</a> , Portecle and KeyStore Explorer.
<b>KPI</b>	Key Performance Indicator
<b>L</b>	
<b>LDAP</b>	<a href="#">Lightweight Directory Access Protocol</a>
<b>LDAP Database</b>	<a href="#">LDAP Concepts and Overview</a>
<b>Load Balancing</b>	<a href="#">Load Balancing and Load Balancing</a>
<b>M</b>	
<b>MAPI</b>	<a href="#">Messaging Application Programming Interface</a>
<b>messageKey</b>	Unique identifier for a message. When a new event with the same messageKey arrives, the old active event is closed.
<b>MOM</b>	Microsoft Operations Manager. See <a href="http://msdn.microsoft.com/en-us/library/aa505337.aspx">http://msdn.microsoft.com/en-us/library/aa505337.aspx</a>
<b>MQ</b>	<a href="#">IBM WebSphere Message Queue</a> middleware for messaging across multiple platforms
<b>MQ Flow</b>	<a href="#">WebSphere MQ server-agent workflow</a>
<b>MySQL Cluster Data Node</b>	<a href="#">MySQL Cluster</a>
<b>MS SQL Database</b>	<a href="#">MS SQL Database tutorial</a> ; also see MS SQL Server
<b>MS SQL Server</b>	<a href="#">Microsoft RDBM</a>
<b>MSMQ Flow</b>	<a href="#">MS Message Queue flow</a> <a href="http://technet.microsoft.com/en-us/library/cc723251.aspx">http://technet.microsoft.com/en-us/library/cc723251.aspx</a>
<b>MySQL Cluster</b>	<a href="#">MySQL Cluster</a>
<b>MySQLClusterDataNode_EntryPoint</b>	<a href="#">Defining MySQL Cluster Data Nodes</a>

<b>MySQLClusterMGM_EntryPoint</b>	<a href="#">MySQL Cluster Management Server</a> <a href="#">MySQL Cluster Management Client</a>
<b>MySQLServer_EntryPoint</b>	<a href="#">MySQLServer</a>
<b>MySQLSlaveServer_EntryPoint</b>	<a href="#">MySQL Server replication</a>
<b>N</b>	
<b>Nagios</b>	An open source network infrastructure monitoring system. Due to trademark problems, the original name, <i>NetSaint</i> , was changed to <i>Nagios</i> , an acronym for "Nagios Ain't Gonna Insist On Sainthood."
<b>NAT</b>	<a href="#">Network Address Translation</a>
<b>nblevent</b>	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/
<b>Netcool</b>	<a href="#">IBM-Tivoli Netcool</a> delivers near real-time, consolidated event management across business infrastructure, data centers, complex networks and IT domains.
<b>netstat</b>	<b>netstat</b> (network statistics) is a <a href="#">command-line tool</a> that displays <a href="#">network connections</a> , <a href="#">routing tables</a> , and network interface ( <a href="#">network interface controller</a> or <a href="#">software-defined network interface</a> ) and network protocol statistics. It is available on <a href="#">Unix-like operating systems</a> including <a href="#">OS X</a> , <a href="#">Linux</a> , <a href="#">Solaris</a> , and <a href="#">BSD</a> , and is available on <a href="#">Windows NT</a> operating systems including <a href="#">Windows XP</a> , <a href="#">Windows Vista</a> , <a href="#">Windows 7 &amp; 8</a> . It finds problems in the network and determines the amount of traffic on the network as a performance measurement.
<b>NNTP</b>	<a href="#">Network News Transfer Protocol</a>
<b>NTLM</b>	<a href="#">NT LAN Manager</a> is a Microsoft Windows security protocol that can be used where a <a href="#">domain controller</a> is not available or is unreachable. For example, NTLM could be used if a client is not <a href="#">Kerberos</a> 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.
<b>O</b>	

<b>OpenSSL</b>	<a href="#">OpenSSL</a> is a toolkit implementing SSL v2/v3 and TLS protocols with full-strength cryptography world-wide.
<b>Oracle Advanced Queue</b>	<a href="#">Oracle Advanced Queuing</a>
<b>Oracle App TNS service</b>	Name by which an Oracle database is known on a network
<b>Oracle Concurrent Server</b>	<a href="#">Concurrent parallel processing</a>
Oracle Database Schema	<a href="#">Oracle Database Schema</a>
Oracle DB	<a href="#">Oracle Database</a>
Oracle Discoverer Engine / UI	<a href="#">Overview of Oracle Discoverer</a>
Oracle E-Business Suite	<a href="#">Overview of Oracle E-Business Suite</a>
Oracle ESB Connection	<a href="#">Oracle Enterprise Service Bus</a>
Oracle Forms Engine / UI	<a href="#">Oracle Forms</a> is a component of Oracle Fusion Middleware
Oracle Fulfillment Server	<a href="#">Oracle Fulfillment Implementation Guide</a>
Oracle HTTP Server	Web server based on the Apache <a href="#">HTTP Server</a>
Oracle iAS Module INC	<a href="#">iAS configuration and tuning</a>
<b>Oracle Linux</b>	<a href="#">Oracle Linux</a> , formerly known as Oracle Enterprise Linux, is a <a href="#">Red Hat Enterprise Linux</a> freely distributed by <a href="#">Oracle</a> under the <a href="#">GNU General Public License</a> (GPL).
Oracle Listener	<a href="#">Oracle Net Listener</a> 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 <a href="#">Oracle Process Manager and Notification Server</a>
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	<a href="#">Oracle Apps Fusion Middleware server</a> runs web services, MapViewer, ASControl, and Oracle Transport Agent XML transactions
Oracle Process Manager	<a href="#">Oracle Process Manager and Notification Server</a>
Oracle RAC DB	<a href="#">Oracle Real Application Clusters database</a>
Oracle Reports Server	<a href="#">Configuring the Oracle Reports Server</a>
Oracle Tnslnsr Engine	<a href="#">TNS Listener, starting and stopping</a>
Oracle WebLogic JMS queue	<a href="#">Oracle WebLogic Java Message Service queue</a>

<b>P</b>	
<b>PEM format</b>	<a href="#">Privacy Enhanced Mail</a> (PEM) is a 1993 <a href="#">IETF</a> proposal for securing email using <a href="#">public-key cryptography</a> .
<b>PeopleSoft Application Server</b>	See BEA Tuxedo (above)
<b>Policy Server</b>	<a href="#">Network Policy Server</a>
<b>POP3</b>	<a href="#">Post Office Protocol</a>
<b>PostgreSQL database</b>	<a href="#">PostgreSQL database</a> Open-source object-relational DBMS supporting SQL constructs incl. subselects, transactions, and user-defined types.
<b>Q</b>	
<b>R</b>	
<b>RAC</b>	<a href="#">Real Application Cluster</a> enables a database to be installed across multiple <a href="#">servers</a> . RAC's method of clustering databases increases <a href="#">scalability</a> (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).
<b>Radware Load Balancer</b>	<a href="#">Radware Load Balancer</a>
<b>Red Hat</b>	<a href="#">Red Hat</a> provides Linux and open source software.
<b>resolutionState</b>	Event resolution state. Values: NEW,CLOSED
<b>RESTful APIs</b>	See <a href="#">RESTful API Design</a> and <a href="#">Representational State Transfer</a>
<b>Reverse collector</b>	Server-initiated collection procedure typically used when the collector cannot initiate a connection because of security considerations.
<b>RFC</b>	<a href="#">Request For Comments</a>
<b>S</b>	
<b>SaaS</b>	<a href="#">Software as a Service</a>
<b>SAP_App_Server_Entry_Point</b>	<a href="#">SAP Application Server</a>
<b>secpol.msc</b>	<a href="#">Local security policy editor</a>
<b>Security Identifier</b>	See SID (below)
<b>ServiceWatch Entry Point</b>	Entry point to the <a href="#">ServiceWatch</a> application

SharePoint connection/portal	<a href="#">URL to the SharePoint site</a>
<b>SID</b>	A <a href="#">Security Identifier</a> is a unique <a href="#">alphanumeric</a> character string assigned by a Windows <a href="#">Domain controller</a> during the log on process. It identifies a user or group of users in a network.
<b>SMTP</b>	<a href="#">Simple Mail Transfer Protocol</a>
Sniffer	A <a href="#">packet analyzer</a> (network analyzer, protocol analyzer, packet sniffer, Ethernet sniffer or wireless sniffer) is software or <a href="#">computer hardware</a> that intercepts and logs traffic passing over a <a href="#">network</a> .
<b>SNMP</b>	<a href="#">Simple Network Management Protocol</a>
<a href="#"><b>Solaris</b></a>	A Unix operating system originally developed by Sun Microsystems. It is now maintained by Oracle.
<b>SolarWinds</b>	<a href="#">SolarWinds</a> Network Performance Monitor detects, diagnoses and resolves network performance problems and outages.
<b>Splunk Enterprise</b>	<a href="#">Splunk Enterprise</a> converts machine data generated by IT systems and technology infrastructure into information about the status of computer networks and applications running on them.
<b>SQL Server Analysis Services</b>	<a href="#">SQL Server Analysis Services</a>
<b>SQL Server Integration</b>	<a href="#">SQL Server Integration Services</a>
<b>SQL Server Reporting</b>	<a href="#">SQL Server Reporting Services</a>
<b>SSAS</b>	<a href="#">SQL Server Analysis Services</a>
<b>SSIS</b>	<a href="#">SQL Server Integration Services</a>
<b>SSIS File EP</b>	<a href="#">SSIS Execute Package file</a>
<b>SSIS Job</b>	<a href="#">SQL Server Integration Services job</a>
<b>SSRS</b>	<a href="#">SQL Server Reporting Services</a>
<b>Storage Array</b>	<a href="#">Disk Array</a>
<a href="#"><b>Stty command</b></a>	This command sets or displays terminal/console settings.
<b>sudo</b>	A program for <a href="#">Unix-like operating systems</a> that allows users to run programs with the security privileges of another user (normally the <a href="#">superuser</a> , or root). Its name is a concatenation of " <a href="#">su</a> " (substitute user) and "do", or take action.
<b>Sun Directory Proxy Server</b>	<a href="#">Sun Directory Proxy Server FAQ</a>
<b>Sun iPlanet Web Server</b>	<a href="#">iPlanet</a>
<b>Sun LDAP Server</b>	<a href="#">Configuring an LDAP Proxy</a>
<a href="#"><b>SUSE</b></a>	An enterprise Linux distribution.
<b>SWaaS</b>	ServiceWatch as a Service (see Chapter 3)
<b>Sybase</b>	<a href="#">Sybase client-server relational database</a>

<a href="#"><b>Symantec NetBackup OpenStorage</b></a>	See also <a href="#">Hitachi Storage systems</a>
<a href="#"><b>Symmetrix</b></a>	EMC Corporation's storage array.
<b>T</b>	
<a href="#"><b>TAM</b></a>	IBM Tivoli Access Manager is an <a href="#">authentication</a> and <a href="#">authorization</a> solution for corporate web services, operating systems, and existing applications. TAM runs on various OSs such as <a href="#">Unix (AIX, Solaris, HP-UX)</a> , <a href="#">Linux</a> , and <a href="#">Microsoft Windows</a> . Like other Tivoli products, it has been renamed as IBM Security Access Manager.
<a href="#"><b>TBS</b></a>	Technical Business Service: A user-specified collection of CIs whose features or connections make it worthwhile to treat them as a group.
<a href="#"><b>TCP</b></a>	<a href="#">Transmission Control Protocol</a>
<a href="#"><b>Tibco</b></a>	<a href="#">Tibco Software</a>
<a href="#"><b>Tibco Active Matrix Business</b></a>	<a href="#">Tibco ActiveMatrix BusinessWorks</a>
<a href="#"><b>Tibco BW</b></a>	<a href="#">Tibco BusinessWorks</a>
<a href="#"><b>Tibco BW process</b></a>	<a href="#">Tibco BW process design guide and concepts</a>
<a href="#"><b>Tibco EMS Queue</b></a>	<a href="#">Tibco Enterprise Message Service routing design</a>
<a href="#"><b>Tibco Enterprise Message</b></a>	<a href="#">Tibco Enterprise Message service</a>
<a href="#"><b>Tibco File Listener</b></a>	<a href="#">Tibco Rendezvous Listener</a>
<a href="#"><b>Tibco Hawk EP</b></a>	<a href="#">Tool for monitoring and managing distributed applications and OSs</a>
<a href="#"><b>Tivoli Netcool</b></a>	See <a href="#">Netcool</a>
<a href="#"><b>TNS</b></a>	Oracle <a href="#">Transparent Network Substrate</a> enables peer-to-peer connectivity where machine-level connectivity cannot occur. It provides a user-transparent layer that enables a heterogeneous network consisting of different protocols to function as a homogeneous network.
<a href="#"><b>Tomcat</b></a>	<a href="#">Apache Tomcat</a>
<a href="#"><b>Tomcat WAR</b></a>	<a href="#">Tomcat Web Archive file</a>
<a href="#"><b>Topology map</b></a>	In the <b>Topology Map</b> screen, ServiceWatch performs a top-down discovery from each entry point defined in the <b>Entry Point</b> screen and displays a <b>Topology Map</b> of the objects in the business service.
<b>U</b>	

<b>Ubuntu</b>	Linux Server operating system. See <a href="http://www.ubuntu.com/">http://www.ubuntu.com/</a>
<b>uCMDB</b>	<a href="#">HP Universal Configuration Management Database</a>
<b>URL</b>	<a href="#">Uniform Resource Locator</a>
<b>V</b>	
<b>vCenter Server</b>	<a href="#">Virtual Server</a>
<b>Virtual Directory</b>	<a href="#">Virtual Directory</a>
<b>vm uuid</b>	<a href="#">Virtual Machine Universal ID</a>
<b>VMware</b>	<a href="#">Virtual Machine ware</a>
<b>VMware Knowledge Base</b>	The VMware Knowledge Base provides support solutions, error messages, and troubleshooting guides.
<b>vmwVC</b>	<a href="#">vmwVC event codes</a>
<b>VSAM</b>	Virtual storage access method is an <a href="#">IBM DASD</a> file storage <a href="#">access method</a> , first used in the <a href="#">OS/VS1</a> , <a href="#">OS/VS2 Release 1</a> (SVS) and <a href="#">Release 2</a> (MVS) operating systems, later used throughout the <a href="#">Multiple Virtual Storage</a> (MVS) architecture and now in <a href="#">z/OS</a> .
<b>W</b>	
<b>Wallet (Oracle)</b>	<a href="#">Oracle wallet</a> : a mechanism for storing and distributing user names and passwords
<b>wbemtest</b>	A utility for testing and exploring WMI. <a href="#">Link1</a> <a href="#">Link2</a> <a href="#">Link3</a> <a href="#">Link4</a>
<b>WebLogic JMS Server</b>	<a href="#">WebLogic JMS Server configuration</a>
<b>WebLogic Module</b>	<a href="#">Plugins for WebLogic Server</a>
<b>WebLogic PS</b>	WebLogic Portal Server
<b>WebSEAL</b>	Multi-threaded Web server that applies fine-grained security policy to a (Tivoli) Access Manager protected Web object space. <a href="#">WebSEAL</a>
<b>WebSphere</b>	IBM's <a href="#">application and integration middleware</a>
<b>WebSphere EAR</b>	<a href="#">WebSphere Enterprise ARchive</a>
<b>WebSphere ODR</b>	<a href="#">WebSphere On-demand router</a>
<b>WebSphere Portal</b>	<a href="#">WebSphere Portal</a>
<b>wget</b>	<a href="#">Wget</a> retrieves content from <a href="#">web servers</a> and is part of the <a href="#">GNU Project</a> . Its name is derived from <a href="#">World Wide Web</a> and <a href="#">get</a> . It downloads via <a href="#">HTTP</a> , <a href="#">HTTPS</a> & <a href="#">FTP</a> protocols

<b>WMB Flow</b>	<a href="#">WebSphere Message Broker: Configuring flows for monitoring video</a>
<b>WMI</b>	<a href="#">Windows Management Instrumentation</a> 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.
<a href="#"><b>wmic</b></a>	Windows Management Instrumentation Command-line
<b>WS</b>	See WebSphere in this glossary.
<b>X</b>	
<a href="#"><b>Xen</b></a>	An open source virtualization standard. See also <a href="#">XenServer</a>
<b>XenApp or Presentation Server Components</b>	<a href="#">Presentation Server 4.5 and Components</a>
<b>XenApp or Presentation Server EP</b>	XenApp Execute Package
<b>xjc tool</b>	<a href="#">Java tool for XML binding</a>
<b>Y</b>	
<b>Z</b>	

# 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](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
DjAMBgNVBAsTBUp1dHR5MRowGAYDVQQDEXFqZXR0eS5tb3J0YmF5Lm9yZzBcMA0G
CSqGSIB3DQEBAQUAA0sAMEgCQQC5V4oZeVdhhdHqa9L2/ZnKySPWUqqy81riNfAJ
7uALW0kEv/Lt1G34dO0cvVt/PK8/bu4dlolnJx1SpimZbKsFAgMBAAGjga4wgasw
HQYDVR0OBBYEFFV1gbB1XRvUx1UofmifQJS/MCYwMHwGA1UdIwR1MHOAFFV1gbB1
XRvUx1UofmifQJS/MCYwovikVjBUMSYwJAYDVQQKEx1Nb3J0IEJheSBDb25zdWx0
aW5nIFB0eS4gTHRkLjEOMAwGA1UECxMFSmV0dHkxGjAYBgNVBAMTEWpldHR5Lm1v
cnRiYXkub3JnggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADQQA6NkaV
OtXzP4ayzbCgK/qSCmF44jdcARmrXhiXUcXzjxsLjSJEPJojhUdC2LQKy+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

The integration of **ServiceWatch** with **ServiceNow CMDB** transfers ServiceWatch-discovered CIs, attributes, relationships, business services and views to ServiceNow CMDB. This document describes the integration architecture and explains how to install, operate, configure, and tailor the integration for your ServiceNow CMDB implementation.

Other types of ServiceWatch & ServiceNow integration (for example, opening a ServiceNow Incident when ServiceWatch discovers that the status of a service is critical) are described in other documents.

The package for integrating ServiceWatch with ServiceNow CMDB is provided with the Service Watch installation and can be found in the **cmdb\sn** folder of the server installation directory.

The package for integrating ServiceWatch with ServiceNow CMDB works on both the SaaS and On-Premise versions of ServiceWatch. It consists of a batch program that runs at a specified time to synchronize the CIs and business service views in ServiceNow with ServiceWatch-discovered CIs and business services. Because standard web service APIs access both ServiceWatch and ServiceNow, the integration can run in local and cloud environments whenever there is HTTPS connectivity to the environments.

Depending on the parameters provided by the operator when running the integration package, the package will synchronize all of the business services active in ServiceWatch or just a single service.

Accurate up-to-date business service data is required inside ServiceNow for these purposes:

- Understanding the service impact when an incident is reported for a specific CI
- Understanding the service impact of a planned change to a CI
- Understanding the risk to service availability based on proposed changes
- Analyzing current service topology to determine if a disaster recovery plan is adequate

However, instructions about how to use ServiceWatch-generated CI and business service data for these purposes in ServiceNow CMDB is *not* covered in this document.

## Architecture & Functional Overview

The package for integrating ServiceWatch with ServiceNow CMDB is a batch file that runs on a Microsoft Windows server. The integration accesses the ServiceWatch application using the ServiceWatch REST web service API to retrieve all (or the requested) business services and all the CIs and relationships that are part of those business services, including applications, servers, and network devices.

The ServiceWatch-discovered CIs are translated to ServiceNow CI format. The transformation results in CIs that are identical to ServiceNow-discovered components. This CI-to-CI mapping is configurable via metadata configuration files that allow any type of ServiceWatch-discovered CIs, attributes and relationships to be translated and imported as ServiceNow CMDB objects. See [TAILORING THE INTEGRATION](#) on page 275 for details.

After the data is converted to ServiceNow format, the integration package accesses ServiceNow using the ServiceNow Web Services API described in the [SERVICE NOW PRODUCT DOCUMENTATION](#) website.

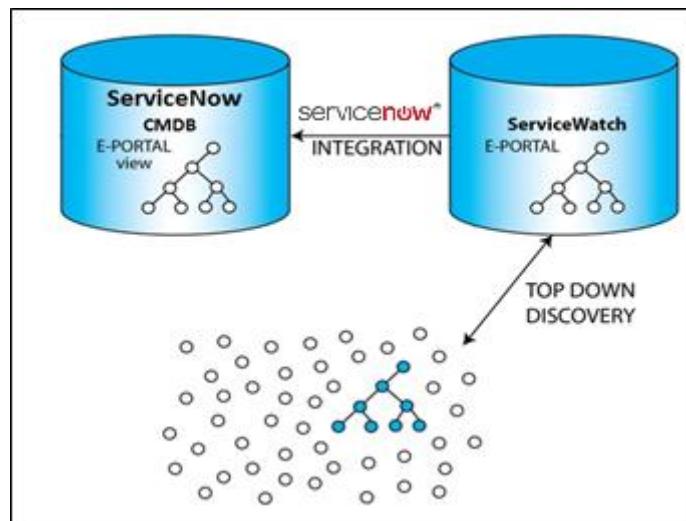
The integration uses the following processes to populate ServiceNow CMDB objects:

- CIs inside ServiceNow CMDB that are part of the business service are identified and marked as business service members by adding the business service name as a Ci attribute.
- The integration checks the relationships in ServiceNow between each CI and its business service. If the ServiceWatch-discovered application flow indicates a change is needed, the relationship is updated and any missing CIs are added in ServiceNow CMDB.
- To enable ServiceNow users to view an accurate up-to-date topological map of the business service, the integration inserts a view of the business service that includes all of its CIs based on the Service ID.

The integration currently supports all major CIs and CI subtypes defined in ServiceNow. The full CI list is in [SUPPLEMENT A: LIST OF SUPPORTED CI TYPES](#). Any CI that does not have a subtype in ServiceNow is tagged as a Generic ServiceNow CMDB CI. You can easily extend support for new CIs by using the metadata configuration file **mapping.xml** as explained in [TAILORING THE INTEGRATION](#) on page 275.

Figure 249 is a graphic illustration of how the ServiceWatch and ServiceNow CMDB integration works. ServiceWatch uses a unique “top-down” discovery method to map the business service and all of its associated CIs. The integration runs as a batch file on a Microsoft Windows server and retrieves business service data from ServiceWatch via a web services API, 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.

Figure 249: Graphic illustration of how the integration works



# ServiceWatch in on-premise mode

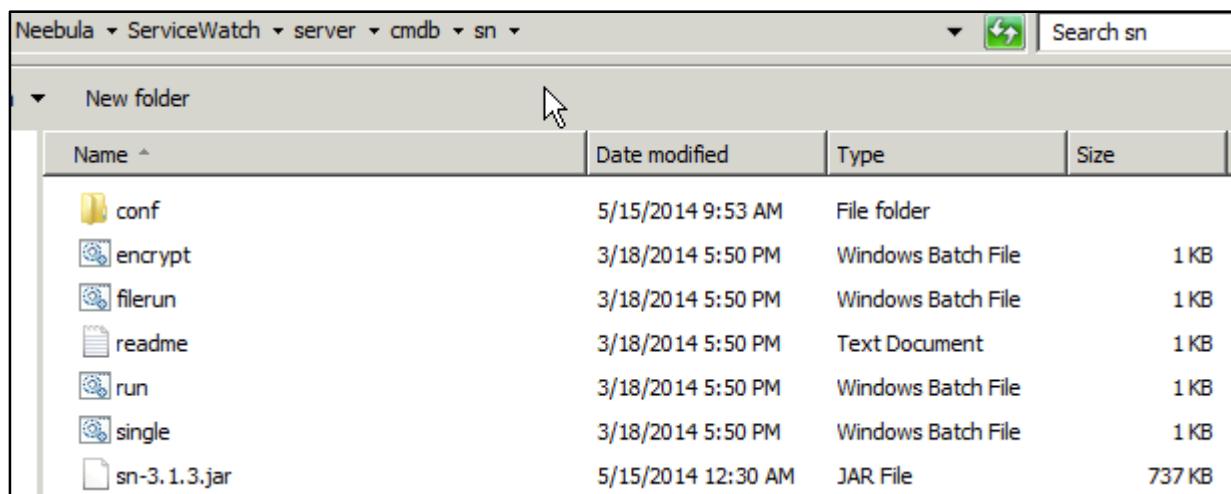
If you are using ServiceWatch as a Service, skip to ServiceWatch as a Service on page 273.

## Installation

The ServiceWatch with ServiceNow CMDB integration files are distributed as part of the ServiceWatch installation package.

1. Navigate to the **Neebula > ServiceWatch > server > cmdb > sn** folder on the same Microsoft Windows server that will run the integration. You should see the following files in that folder:

**Figure 250: Contents of the Neebula > ServiceWatch > server > cmdb > sn folder**



Name	Date modified	Type	Size
conf	5/15/2014 9:53 AM	File folder	
encrypt	3/18/2014 5:50 PM	Windows Batch File	1 KB
filerun	3/18/2014 5:50 PM	Windows Batch File	1 KB
readme	3/18/2014 5:50 PM	Text Document	1 KB
run	3/18/2014 5:50 PM	Windows Batch File	1 KB
single	3/18/2014 5:50 PM	Windows Batch File	1 KB
sn-3.1.3.jar	5/15/2014 12:30 AM	JAR File	737 KB

2. Use the **encrypt.bat** file to produce the two encrypted passwords that are in the **config.properties** file. The only parameter for the **encrypt.bat** command is the unencrypted password. The output is a 50-character encrypted password. For example:  

```
C:\neebula\servicewatch\collector\cmdb\sn>encrypt.bat mypassword
Encrypted key:< 50-character encrypted password >
```

## On-Premise Configuration

3. Specify values for the parameters in the **config.properties** file.
  - Set **sn\_uname** to a ServiceNow username with admin authority.
  - Set **sn\_password** to that username's 50-character encrypted password.
  - Set **sn\_url** to the URL of your ServiceNow instance.
  - Set **neebula\_uname** to an administrator user of your ServiceWatch application.
  - Set **neebula\_password** to the 50-character Encrypted key for that administrator user.
  - Set **neebula\_url** to your ServiceWatch server url.
  - When the **create\_hosts** and **network** parameters are set to **true**, they direct the integration to add hosts and network devices if they so not already exist in

ServiceNow CMDB. CIs and relationships are automatically created if they do not already exist in ServiceNow CMDB and their hosts do exist.

- **business\_service\_rel\_attr** specifies the ServiceNow attribute name that contains the names of the Business Services.

4. After setting values in the **config.properties** file, it will look similar to:

```
sn_uname=haviv
sn_password=3ZidHE/MGm55Lx0v4BUY4g==| |MBks2t0Zod2yV6Y369SPpg==
sn_url=https://dev009.service-now.com/
neebula_uname=admin
neebula_password=liup8q+5+PH8i6hJ7W56rQ==| |PKFog4U4LheDp3xt5YU5bQ==
neebula_url=http://localhost:8080/ws/bss
#apikey is relevant for Neebula saas customers only
apikey=
create_hosts=true
network=false
business_service_rel_attr=attributes
```

5. Save the **config.properties** file. Configuration of ServiceWatch with ServiceNow CMDB integration is complete.

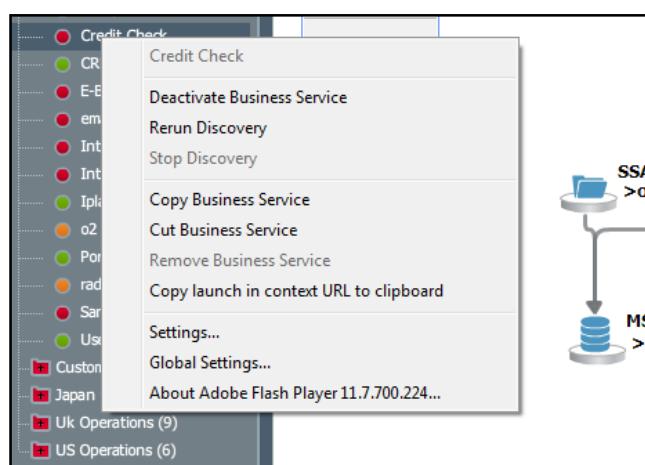
6. The **run.bat** and **single.bat** files can be scheduled to run at a suitable time based on your update policy:

- **run.bat** has no configurable parameters. It copies all active ServiceWatch-discovered business services to ServiceNow CMDB.
- **single.bat** receives one parameter whose value is an integer that identifies a specific business service. The integration package will populate only this business service, including all of its CIs, in ServiceNow CMDB. The syntax is: **single.bat < Business Service ID # >**

For example, **single.bat 1234**

To obtain the Business Service ID number, right click the desired Business Service in the **Active** tree and select **Copy launch in context URL to clipboard** in the pop-up menu. See the **config.properties** and **mapping.xml** files for credentials and advanced mapping settings.

**Figure 251: Business Service right-click pop-up menu**



The clipboard now contains a URL similar to

<http://localhost:8080/ui/?screen=monitor&bsid=nnnn>

Copy the integer after bsid= from the clipboard and use it as the parameter value for the single.bat command. When you run the **single.bat** command, the business service whose number you specified, including its CIs, is added to or modified in ServiceNow.

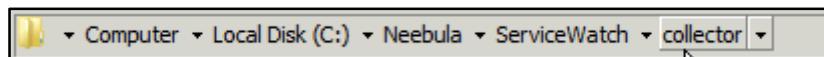
Skip to Tailoring the Integration on page [275](#).

## ServiceWatch as a Service (SWaaS)

If you are using ServiceWatch in on-premise mode, run the installation and configuration steps in ServiceWatch in on-premise mode on page [271](#), then skip to Tailoring the Integration on page [275](#).

## Installation

1. Obtain the ServiceWatch with ServiceNow CMDB installation zip file from the ServiceWatch support team.
2. Create the **cmdb** folder in the **Neebula > ServiceWatch > collector** path on the same Microsoft Windows server that will run the integration.



3. Extract the compressed files. The extraction should create a **sn** folder that contains the following subfolder and files.

**Figure 252: List of extracted files**

Name	Date modified	Type	Size
conf	5/21/2014 10:16 AM	File folder	
encrypt	3/18/2014 5:50 PM	Windows Batch File	1 KB
filerun	3/18/2014 5:50 PM	Windows Batch File	1 KB
readme	3/18/2014 5:50 PM	Text Document	1 KB
run	3/18/2014 5:50 PM	Windows Batch File	1 KB
single	3/18/2014 5:50 PM	Windows Batch File	1 KB
sn-3.1.3.jar	5/15/2014 12:30 AM	JAR File	737 KB

4. Use the **encrypt.bat** file to produce the two encrypted passwords that are in the **config.properties** file. The only parameter for the **encrypt.bat** command is the unencrypted password. The output is a 50-character encrypted password. For example:
- ```
C:\neebula\servicewatch\collector\cmdb\sn>encrypt.bat mypassword
Encrypted key:< 50-character encrypted password >
```

## SWaaS Configuration

5. Specify values for the parameters in the **config.properties** file.
  - Set **sn\_uname** to a ServiceNow username with admin authority.
  - Set **sn\_password** to that username's 50-character encrypted password.
  - Set **sn\_url** to the URL of your ServiceNow instance.
  - Leave the **neebula\_uname** value empty (null).
  - You can leave **neebula\_password** as it is. The **apikey** is used to authenticate against the ServiceWatch as a Service server.
  - Do not change the **neebula\_url** setting. It should point to <https://saas.neebula.com/ws/bss>
  - Set **apikey** to the value obtained from the ServiceWatch Operations Center.
  - When the **create\_hosts** and **network** parameters are set to **true**, they direct the integration to add hosts and network devices if they so not already exist in ServiceNow CMDB. CIs and relationships are automatically created if they do not already exist in ServiceNow CMDB and their hosts do exist.
  - **business\_service\_rel\_attr** specifies the ServiceNow attribute name that contains the names of the Business Services.

6. After setting values in the **config.properties** file, it will look similar to:

```

sn_uname=haviv
sn_password=3ZiDHE/MGm55Lx0v4BUY4g==|MBks2t0zod2yV6Y369SPpg==
sn_url=https://dev009.service-now.com/
neebula_uname=
neebula_password=liup8q+5+PH8i6hJ7W56rQ==|PKFog4U4LheDp3xt5YU5bQ==
neebula_url=https://saas.neebula.com/ws/bss
#apikey is relevant for Neebula saas customers only
apikey=YbJb9FTSds4S56L7NFGae2
create_hosts=true
network=false
business_service_rel_attr=attributes
  
```

7. Save the **config.properties** file. Configuration of the ServiceWatch with ServiceNow CMDB integration is complete.
8. The **run.bat** and **single.bat** files can be scheduled to run at a suitable time based on your update policy:
  - **run.bat** has no configurable parameters. It copies all ServiceWatch-discovered business services to ServiceNow CMDB.
  - **single.bat** receives one parameter whose value is an integer that identifies a specific business service. The integration package will populate only this business service, including all of its CIs, in ServiceNow CMDB. The syntax is: **single.bat < Business Service ID # >**  
For example, **single.bat 1234**

To obtain the Business Service ID number, right click the desired Business Service in the **Active** tree and select **Copy launch in context URL to clipboard** in the pop-up menu (see Figure 251: Business Service right-click pop-up menu).

The clipboard now contains a URL similar to

<http://localhost:8080/ui/?screen=monitor&bsid=nnnn>

Copy the integer after bsid= from the clipboard and use it as the parameter value for the single.bat command. When you run the **single.bat** command, the business service whose number you specified, including its CIs, is added to or modified in ServiceNow.

## Tailoring the Integration

The integration of ServiceWatch with ServiceNow CMDB is very flexible. It can be modified to add any CI or relationship, CI Key, or CI identification algorithm. These capabilities will be available in the ServiceWatch release GA release scheduled for April 2014. For most users, no changes will be required to any of the default configurations.

The following paragraphs explain how to change the mapping in the integration. For additional help, contact the ServiceWatch Operations Center.

The **mapping.xml** file in the **orchestrator-server > cmdb > sn > conf** directory controls how the ServiceWatch with ServiceNow CMDB integration works.

## Deleting/Changing/Adding ServiceWatch CIs & Relationships in ServiceNow

Locate the following section of the **mapping.xml** file. It contains the list of ServiceNow relationships and CIs handled by the integration. All non-defined CIs are mapped to a Generic CI in the ServiceNow CMDB.

The process for converting attributes and keys and binding them to the CMDB has been specified for each defined CI. To add a new CI to the ServiceWatch integration, first display its xml in ServiceNow and then copy its CI name (such as `cmdb_ci_computer`) and add it to this list.

```

<bean id="Mappings" class="java.util.ArrayList">
    - <constructor-arg>
        - <list>
            <ref bean="cmdb_ci_app_server_websphere" />
            <ref bean="cmdb_ci_app_server_weblogic" />
            <ref bean="cmdb_ci_app_server_jboss" />
            <ref bean="cmdb_ci_app_server_tomcat" />
            <ref bean="cmdb_ci_app_server_oracle" />
            <ref bean="cmdb_ci_database" />
            <ref bean="cmdb_ci_web_server" />
            <ref bean="cmdb_ci_linux_server" />
            <ref bean="cmdb_ci_unix_server" />
            <ref bean="cmdb_ci_aix_server" />

```

```

<ref bean="cmdb_ci_hpxx_server" />
<ref bean="cmdb_ci_win_server" />
<ref bean="cmdb_ci_solaris_server" />
<ref bean="network_gear" />
<ref bean="dependsOn" />
<ref bean="connectedTo" />
<ref bean="runsOn" />
<ref bean="business_service" />
<ref bean="AllOther" />
</list>

```

## Mapping ServiceWatch-Discovered CIs to ServiceNow CIs

The ServiceWatch with ServiceNow CMDB integration contains an XML representation that enables the default procedures for converting and binding CIs to be changed. 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. In addition, the following attributes are automatically populated and available for conversion for each ServiceWatch CI.

**Note:** The attribute name below is the same 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<br>(example:<br><a href="http://(neebula)/ui/?screen=physical&amp;ciid=8763">http://(neebula)/ui/?screen=physical&amp;ciid=8763</a> ) |
| version                      | Version of the software including patch level                                                                                                                                                                                                                                      |
| label                        | Name of the application                                                                                                                                                                                                                                                            |
| description                  | Description entered by the user                                                                                                                                                                                                                                                    |
| typeName                     | Type of CI in ServiceWatch                                                                                                                                                                                                                                                         |
| bsId                         | List of numbers (IDs) separated by ‘,’ of the business services to which the CI belongs                                                                                                                                                                                            |
| bsName                       | List of names separated by ‘,’ of the business services the CI supports                                                                                                                                                                                                            |
| 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                                                                                                                                                                                                                                                                               |
| host.Primary_host_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           |                                                                                                                                                                                                                                                                                    |
| type                         | represents connection type (HTTP, TCP, etc.)                                                                                                                                                                                                                                       |

In addition, all specific CI Type attributes (as defined in the ServiceWatch CI) are available as seen in the following screen for Microsoft SQL:

**Figure 253: Table of CI Attributes in the CI Type Definition screen**

| Name                         | Description                 | Display Name                 | Type   | Key | Required | Editable | Searchable |
|------------------------------|-----------------------------|------------------------------|--------|-----|----------|----------|------------|
| alternate_label              | GUI alternate display label | Alternate Label              | String |     |          | ✓        | ✓          |
| app_processes                |                             | Application Processes        | Table  |     |          |          | ✓          |
| app_services                 |                             | Application Services         | Table  |     |          |          | ✓          |
| extended_attr                |                             | Extended Attributes          | Table  |     |          |          | ✓          |
| install_dir                  | Installed Directory         | Installation directory       | String |     | ✓        |          | ✓          |
| label                        | GUI display label           | Label                        | String |     |          |          | ✓          |
| location                     |                             | Location                     | String |     |          | ✓        | ✓          |
| processes_with_creation_time |                             | Processes with creation time | Table  |     |          |          | ✗          |
| queue_manager                | Queue Manager Name          | Queue manager name           | String | ✓   | ✓        |          | ✓          |
| tracked_files                |                             | Tracked Files                | Table  |     |          |          | ✗          |
| version                      | mq version                  | Version                      | String |     |          | ✓        | ✗          |

To determine possible candidates for attributes in the ServiceNow CMDB, look at the XML that defines the CI Type in ServiceNow.

## Mapping a ServiceWatch-Discovered WebSphere to ServiceNow

How **java.util.ArrayList** defines which CIs are converted is described in [DELETING/CHANGING/ADDING SERVICEWATCH CIs & RELATIONSHIPS IN SERVICENOW](#) on page 275.

How CI attributes are translated is described here.

For each CI in **java.util.ArrayList**, the XML below maps a ServiceWatch-discovered CI to a ServiceNow CI. Each ServiceWatch-discovered attribute overrides the corresponding attribute of the matching ServiceNow CI. The default is to map only required attributes in order to minimize changes to the ServiceNow CMDB.

## CI Attribute Translation

```

<bean id="cmdb_ci_app_server_websphere"

class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebul
aMapping">

    <!--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"/>

    <property name="cmdbService"
ref="cmdb_ci_app_server_websphere_Service"/>

    <!--
           mappingRules contain a list of rules that populate the
CMDB CIT attributes.

           The key represents the CMDB attribute name and the value
should contain an expression
           that defines the desired value. The expression may
contain these operators/operators:
           + for concatenation
           ${attName} - represents an attribute value: for example
           ${version} returns the value of the version
attribute on Neebula CI
           '' - for constants
           For additional transformation capabilities, see
http://groovy.codehaus.org/User+Guide
-->
    <property name="mappingRules">
        <map key-type="java.lang.String" value-
type="java.lang.String">
            <entry key="Version" value="${version}" />
            <entry key="Name"
value="${label}+'@'+${host.Primary_host_name_or_ip}" />
            <entry key="shortDescription" value="${description}" />
        </map>
    </property>
    <!--
           KeyRules contains a list of matching rules used to locate a
specific instance on the CMDB side.

           It is basically the integration identify matching rules for
the specific CIT.
-->
    <property name="keyRules" ref="AliasRule" />

</bean>

```

## Sample XML for CI-to-CI mapping

```

<property name="cmdbCIT" value="cmdb_ci_app_server_websphere"/> - Name of the ServiceNow CI Type
<property name="neebulaCIT" value="Websphere"/>

<property name="mappingRules">
<map key-type="java.lang.String" value-type="java.lang.String">
String
<entry key="Version" value="${version}"/>

<property name="keyRules">

`<bean id="AliasRule" class="java.util.ArrayList">
<constructor-arg>
    <list value-type="com.doitwise.neebula.utils.Pair">
        <bean class="com.doitwise.neebula.utils.Pair">
            <property name="first" value="Name"></property>
            <property name="second" value="${label}@'${host.Primary_host_name}'></property>
        </bean>
        <bean class="com.doitwise.neebula.utils.Pair">
            <property name="first" value="Name"></property>
            <property name="second" value="${label}@'${host.Primary_management_IP}'></property>
        </bean>
    </list>
</constructor-arg>
</bean>
compare
This rule tells the integration to first
the Serial number, then the host name, and
finally the IP.

```

## Mapping ServiceWatch Relationships

Mapping relationships is performed after ServiceWatch-discovered CIs have been incorporated in ServiceNow CMDB. The integration activates the relationships section for each ServiceWatch-discovered CI if there is a matching CI in the ServiceNow CMDB. The integration sets these ServiceNow variables to appropriate values.

| Variable    | Description                     |
|-------------|---------------------------------|
| src.id      | ServiceNow ID of the source CI  |
| src.type    | Type of source CI in ServiceNow |
| target.id   | ID of target CI in ServiceNow   |
| target.type | Type of target CI in ServiceNow |

### Relationship mapping example

```
<bean id="connectedTo"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping">
  <property name="handler"
    value="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationHandler"/>
  <property name="cmdbCIT" value="cmdb_rel_ci"/>
  <property name="neebulaCIT" value="RELATION_BSS_MEMBER"/>
  <property name="mappingRules">
    <map key-type="java.lang.String" value-type="java.lang.String">
      <entry key="Type" value="<one of the available types>"/>
        The available types are:
        5599a965c0a8010e00da3b58b113d70e → connectedT
        o
        1 → dependsOn
        60bc4e22c0a8010e01f074cbe6bd73c3 → runsOn
      <entry key="Parent" value="${src.id}"/>
      <entry key="Child" value="${target.id}"/>
    </map>
  </property>
</bean>
```

### Relationship mapping explanation

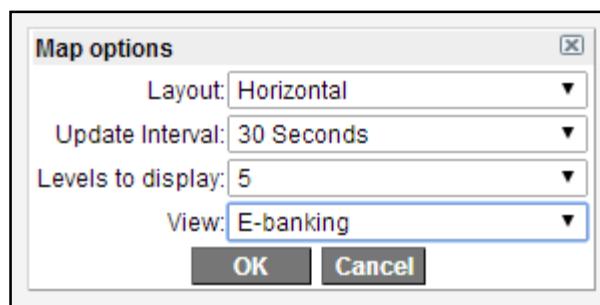
|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bean id="connectedTo"                              | Name of the ServiceNow relationship. This is a human readable description of the ServiceNow relationship type represented by a large key labeled "Type". If adding a new relationship, update this value.                                                                                                                                                                                                                                        |
| name="cmdbCIT" value="cmdb_rel_ci"<br>relationship | Modified to indicate a ServiceNow                                                                                                                                                                                                                                                                                                                                                                                                                |
| name="neebulaCIT" value="RELATION_BSS_MEMBER"      | ServiceWatch relationship type. If this CI is part of a business service, ServiceWatch translates the relationship to a ServiceNow 'Connected_To' relationship. However, it does not connect it to the business service CI. Only the first top CI is connected to the business service. This enables the user to view the real topology of the service by selecting the business service and then selecting view with the business service name. |

|                                                   |                                                                                                                                |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| "Type" value=""5599a965c0a8010e00da3b58b113d70e"" | Key of the ServiceNow relationship type<br>(see <a href="#">VIEWING SERVICEWATCH-DISCOVERED SERVICE MODELS IN SERVICENOW</a> ) |
| entry key="Parent" value="\${src.id}"             | Setting the ServiceNow Parent Attribute                                                                                        |
| entry key="Child" value="\${target.id}"           | Setting the ServiceNow Child Attribute                                                                                         |

## Viewing ServiceWatch-Discovered Service Models in ServiceNow

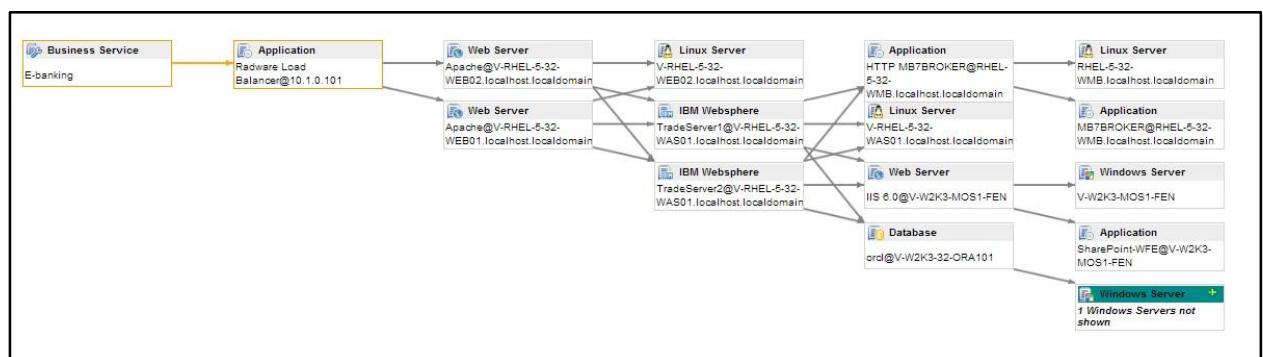
Business Service Member relationship types do not exist in the ServiceNow CMDB. To simulate the ServiceWatch service model viewing capabilities, the integration by default creates a CI for each business service and connects it (with a standard **connectedTo** relationship) to the first-tier CI of the business service (the entry point). In the following example, ServiceWatch discovers the Radware load balancer and adds the name and the ID of the service to each subsequent CI as discovered (as a component comprising the service). In addition, a view is added under the name of the business service (in this case e-Banking) which only selects the CIs associated with that service. The result is:

[Figure 254: Map options dialog box for E-banking View](#)



The actual topology and application flow of the business service becomes visible in ServiceNow:

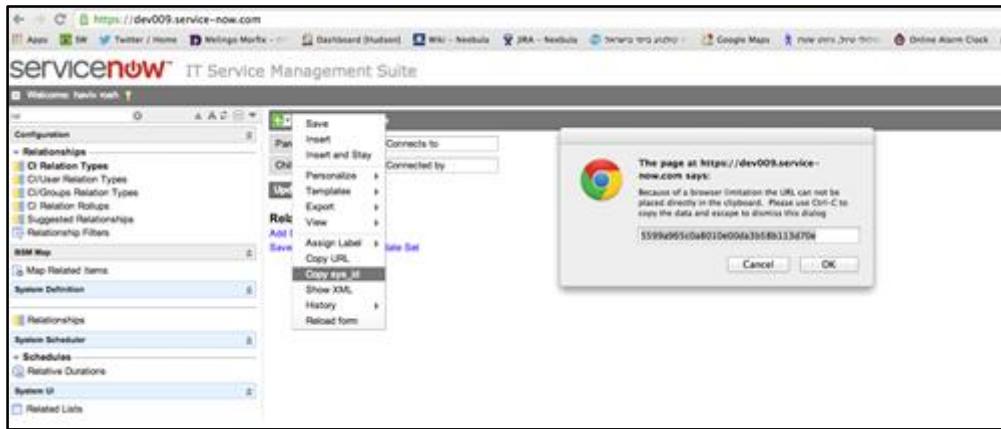
[Figure 255: E-banking Business Service as displayed in ServiceNow](#)



## Determining the Relationship Type Key

To determine the Key of the relationship type you want to populate, visit the ServiceNow website and extract the Key as shown in the following image:

Figure 256: ServiceNow Key extraction



## 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.

## Supplement A: List of Supported CI Types

All CIs supported by the integration are defined in the **mapping.xml** file in the main directory. New CIs can be easily added and mapped to the integration. See [TAILORING THE INTEGRATION](#) on page 275 for details. The default definition for the attributes associated with the following CIs and relationships is the same format used for ServiceNow discovery.

- Application Servers:
  - ✓ cmdb\_ci\_app\_server\_websphere
  - ✓ cmdb\_ci\_app\_server\_weblogic
  - ✓ cmdb\_ci\_app\_server\_jboss
  - ✓ cmdb\_ci\_app\_server\_tomcat
  - ✓ The rest are mapped to cmdb\_ci\_app\_server
- Database Servers:
  - ✓ cmdb\_ci\_database with one of the next type attributes:
    - Oracle
    - DB2
    - Microsoft Sql Server
    - MySQL
    - Postgres SQL
    - Sybase
- Web Servers:
  - ✓ cmdb\_ci\_web\_server with one of the next type attributes:
    - Apache
    - iPlanet
    - Microsoft-IIS
- Hosts:
  - ✓ cmdb\_ci\_linux\_server
  - ✓ cmdb\_ci\_unix\_server
  - ✓ cmdb\_ci\_aix\_server
  - ✓ cmdb\_ci\_hpxu\_server
  - ✓ cmdb\_ci\_win\_server
  - ✓ cmdb\_ci\_solaris\_server
- Network gear
  - ✓ cmdb\_ci\_ip\_router
  - ✓ cmdb\_ci\_ip\_switch
- All other applications will be mapped to cmdb\_ci\_appl

## Supplement B: Default Installation mapping.xml file

The complete XML code in the **mapping xml** file of the ServiceWatch with ServiceNow CMDB integration package is listed below. This listing is provided for reference only and is intended to show how each attribute is translated and transferred to ServiceNow CMDB by this out-of-the-box integration package. This code may change, so use the copy provided with your installation. If the **mapping xml** file is updated to tailor the integration, remember to back up your custom tailored file when upgrading to ensure that the new version works properly in your environment and produces the desired results.

```

<?xml version="1.0" encoding="UTF-8" ?>
- <beans xmlns="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/beans
  http://www.springframework.org/schema/beans/spring-beans-3.0.xsd">
- <bean id="MappingHandler"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.MappingHandler"
  scope="singleton">
<property name="mappingList" ref="Mappings" />
</bean>
<bean id="cmdb_ci_app_server_websphere_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.AppServerService"
  scope="singleton" />
<bean id="cmdb_ci_app_server_weblogic_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.AppServerService"
  scope="singleton" />
<bean id="cmdb_ci_app_server_jboss_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.AppServerService"
  scope="singleton" />
<bean id="cmdb_ci_app_server_tomcat_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.AppServerService"
  scope="singleton" />
<bean id="cmdb_ci_app_server_oracle_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.AppServerService"
  scope="singleton" />
<bean id="cmdb_ci_database_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.DBServerService"
  scope="singleton" />
<bean id="cmdb_ci_web_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.WebServerService"
  scope="singleton" />
<bean id="cmdb_ci_linux_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemService"
  scope="singleton" />
<bean id="cmdb_ci_aix_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemService"
  scope="singleton" />
<bean id="cmdb_ci_unix_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemService"
  scope="singleton" />
<bean id="cmdb_ci_hpxu_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemService"
  scope="singleton" />
<bean id="cmdb_ci_win_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemService"
  scope="singleton" />
<bean id="cmdb_ci_solaris_server_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemService"
  scope="singleton" />
<bean id="cmdb_ci_ip_router_Service"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.NetworkGearService"
  scope="singleton" />
```

```

<bean id="cmdb_ci_ip_switch_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.NetworkGearService"
scope="singleton" />
<bean id="dependsOn_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationService"
scope="singleton" />
<bean id="connectedTo_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationService"
scope="singleton" />
<bean id="runsOn_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationService"
scope="singleton" />
<bean id="business_service_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.BusinessServiceService"
scope="singleton" />
<bean id="network_gear_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.NetworkGearService"
scope="singleton" />
<bean id="generic_app_Service"
class="com.neebula.orchestrator.integration.cmdb.sn.handler.GenericAppServerService"
scope="singleton" />
- <!--
    This list represents the Neebula to CMDB integration mapping: each mapping
represents mapping of a specific
    CMDB CIT

-->
- <bean id="Mappings" class="java.util.ArrayList">
- <constructor-arg>
- <list>
<ref bean="cmdb_ci_app_server_websphere" />
<ref bean="cmdb_ci_app_server_weblogic" />
<ref bean="cmdb_ci_app_server_jboss" />
<ref bean="cmdb_ci_app_server_tomcat" />
<ref bean="cmdb_ci_app_server_oracle" />
<ref bean="cmdb_ci_database" />
<ref bean="cmdb_ci_web_server" />
<ref bean="cmdb_ci_linux_server" />
<ref bean="cmdb_ci_unix_server" />
<ref bean="cmdb_ci_aix_server" />
<ref bean="cmdb_ci_hpxx_server" />
<ref bean="cmdb_ci_win_server" />
<ref bean="cmdb_ci_solaris_server" />
<ref bean="network_gear" />
<ref bean="dependsOn" />
<ref bean="connectedTo" />
<ref bean="runsOn" />
<ref bean="business_service" />
<ref bean="AllOther" />
</list>
</constructor-arg>
</bean>
- <!--
    CIT Mapping Rules
    Available ServiceWatch 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.OS_Type - operating system name
host.OS_Version
host.Model
host.Domain
host.Address_Width
type - represents the connection type (HTTP, TCP, etc...)

*application specific attributes per ServiceWatch CIT are also available (for
example instance in all data base servers)

-->
- <!--
=====
Application Servers
=====

-->
- <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
multiple CIT with , as delimiter between them
-->
<property name="neebulaCIT" value="Websphere" />
<property name="cmdbService" ref="cmdb_ci_app_server_websphere_Service" />
- <!--
      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 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="Version" value="${version}" />
<entry key="Name" value="${label}'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</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 identify matching rules for this
      specific CIT.

-->
<property name="keyRules" ref="AliasRule" />
</bean>
- <bean id="cmdb_ci_app_server_weblogic"
  class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping"
  ">
<property name="cmdbCIT" value="cmdb_ci_app_server_weblogic" />
<property name="neebulaCIT" value="Weblogic" />
<property name="cmdbService" ref="cmdb_ci_app_server_weblogic_Service" />
- <property name="mappingRules">
```

```

- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Version" value="${version}" />
<entry key="Name" value="${label}'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</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 identify matching rules for this
      specific CIT.

-->
<property name="keyRules" ref="AliasRule" />
</bean>
- <bean id="cmdb_ci_app_server_jboss"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_app_server_jboss" />
<property name="neebulaCIT" value="Jboss" />
<property name="cmdbService" ref="cmdb_ci_app_server_jboss_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Version" value="${version}" />
<entry key="Name" value="${label}'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</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 identify matching rules for this
      specific CIT.

-->
<property name="keyRules" ref="AliasRule" />
</bean>
- <bean id="cmdb_ci_app_server_oracle"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_app_server" />
<property name="neebulaCIT" value="Oracle iAS" />
<property name="cmdbService" ref="cmdb_ci_app_server_oracle_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Version" value="${version}" />
<entry key="Name" value="${label}'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</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 identify matching rules for this
      specific CIT.

-->
<property name="keyRules" ref="AliasRule" />
</bean>
- <bean id="cmdb_ci_app_server_tomcat"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_app_server" />
<property name="neebulaCIT" value="Tomcat" />
<property name="cmdbService" ref="cmdb_ci_app_server_tomcat_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Version" value="${version}" />

```

```

<entry key="Name" value="${label}+'@'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</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 identify matching rules for this
    specific CIT.

-->
<property name="keyRules" ref="AliasRule" />
</bean>
- <!--
=====
Web Servers
=====

-->
- <bean id="cmdb_ci_web_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_web_server" />
<property name="neebulaCIT" value="Apache,IIS,iplanet" />
<property name="cmdbService" ref="cmdb_ci_web_server_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Version" value="${version}" />
<entry key="Name" value="${label}+'@'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</map>
</property>
<property name="keyRules" ref="AliasRule" />
</bean>
- <!--
=====
DB Servers
=====

-->
- <bean id="cmdb_ci_database"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_database" />
<property name="neebulaCIT" value="Oracle DB,MS SQL server,PostgreSQL
DB,MySQLServer,Sybase,DB2" />
<property name="cmdbService" ref="cmdb_ci_database_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Version" value="${version}" />
<entry key="Name" value="${label}+'@'+${host.Primary_host_name}" />
<entry key="shortDescription" value="${description}" />
</map>
</property>
<property name="keyRules" ref="AliasRule" />
</bean>
- <!--
=====
Hosts
=====

-->
- <bean id="cmdb_ci_linux_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_linux_server" />
<property name="neebulaCIT" value="host" />
<property name="matchingRule" value="${OS_Type} == 'LINUX' || ${OS_Family} ==
'PROPRIETARY'" />

```

```

<property name="handler"
value="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemHandler"
/>
<property name="cmdbService" ref="cmdb_ci_linux_server_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />
<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="shortDescription" value="${Description}" />
<entry key="Os" value="Linux'" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <bean id="cmdb_ci_unix_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_unix_server" />
<property name="neebulaCIT" value="host" />
<property name="matchingRule" value="${OS_Type} == 'UNIX'" />
<property name="handler"
value="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemHandler"
/>
<property name="cmdbService" ref="cmdb_ci_unix_server_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />
<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="Os" value="Unix'" />
<entry key="shortDescription" value="${Description}" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <bean id="cmdb_ci_aix_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_aix_server" />
<property name="neebulaCIT" value="host" />
<property name="matchingRule" value="${OS_Type} == 'AIX'" />
<property name="handler"
value="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemHandler"
/>
<property name="cmdbService" ref="cmdb_ci_aix_server_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />
<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="shortDescription" value="${Description}" />
<entry key="Os" value="Aix'" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <bean id="cmdb_ci_hpxu_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_hpxu_server" />
<property name="neebulaCIT" value="host" />
<property name="matchingRule" value="${OS_Type} == 'HPUX'" />
<property name="handler"
value="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemHandler"
/>
<property name="cmdbService" ref="cmdb_ci_hpxu_server_Service" />
- <property name="mappingRules">

```

```

- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />
<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="shortDescription" value="${Description}" />
<entry key="Os" value="'HPUX'" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <bean id="cmdb_ci_win_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_win_server" />
<property name="neebulaCIT" value="host" />
<property name="matchingRule" value="${OS_Type}.contains('WINDOWS')" />
<property name="handler"
          value="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemHandler"
          />
<property name="cmdbService" ref="cmdb_ci_win_server_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />
<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="shortDescription" value="${Description}" />
<entry key="Os" value="Windows'" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <bean id="cmdb_ci_solaris_server"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_solaris_server" />
<property name="neebulaCIT" value="host" />
<property name="matchingRule" value="${OS_Type}.contains('SOLARIS')" />
<property name="handler"
          value="com.neebula.orchestrator.integration.cmdb.sn.handler.ComputerSystemHandler"
          />
<property name="cmdbService" ref="cmdb_ci_solaris_server_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />
<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="shortDescription" value="${Description}" />
<entry key="Os" value="Solaris'" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <!--
=====
Network Gear Mapping
=====

-->
- <bean id="network_gear"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci" />
<property name="neebulaCIT" value="Network Device" />
<property name="handler"
          value="com.neebula.orchestrator.integration.cmdb.sn.handler.NetworkGearHandler" />
<property name="cmdbService" ref="network_gear_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${host.Primary_host_name}" />

```

```

<entry key="serialNumber" value="${Serial_number}" />
<entry key="IpAddress" value="${Primary_management_IP}" />
<entry key="shortDescription" value="${Description}" />
</map>
</property>
<property name="keyRules" ref="ComputerSystemMatchingRule" />
</bean>
- <!--
=====
Business Service Mapping
=====

-->
- <bean id="business_service"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_service" />
<property name="neebulaCIT" value="BUSINESS_SERVICE" />
<property name="cmdbService" ref="business_service_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${label}" />
<entry key="shortDescription" value="${description}" />
</map>
</property>
<property name="keyRules" ref="BusinessServiceMatchingRule" />
</bean>
- <!--
=====
All other applications will be mapped as generic ci
=====

-->
- <bean id="AllOther"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="cmdbCIT" value="cmdb_ci_appl" />
<property name="neebulaCIT" value="*" />
<property name="handler"
      value="com.neebula.orchestrator.integration.cmdb.sn.handler.GenericAppServerHandler
      " />
<property name="cmdbService" ref="generic_app_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Name" value="${label}#{@${host.Primary_host_name}}" />
<entry key="shortDescription" value="${description}" />
<entry key="Type" value="${typeName}" />
</map>
</property>
<property name="keyRules" ref="AliasRule" />
</bean>
- <!--
Relations Mapping Rules
available attributes to use:
src.id
src.type
target.id
target.type
type - represents the connection type (HTTP, TCP, etc...)
=====

-->
- <bean id="dependsOn"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="handler"
      value="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationHandler" />
<property name="cmdbCIT" value="cmdb_rel_ci" />
<property name="neebulaCIT" value="APPLICATION_FLOW,CLUSTER" />
<property name="cmdbService" ref="dependsOn_Service" />
- <property name="mappingRules">

```

```

- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Type" value="1" />
<entry key="Parent" value="${src.id}" />
<entry key="Child" value="${target.id}" />
</map>
</property>
</bean>
- <bean id="runsOn"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="handler"
value="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationHandler" />
<property name="cmdbCIT" value="cmdb_rel_ci" />
<property name="neebulaCIT" value="INCLUSION" />
<property name="cmdbService" ref="runsOn_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Type" value="60bc4e22c0a8010e01f074cbe6bd73c3'" />
<entry key="Child" value="${target.id}" />
<entry key="Parent" value="${src.id}" />
</map>
</property>
</bean>
- <bean id="connectedTo"
      class="com.neebula.orchestrator.integration.cmdb.sn.handler.CMDBToNeebulaMapping
      ">
<property name="handler"
value="com.neebula.orchestrator.integration.cmdb.sn.handler.RelationHandler" />
<property name="cmdbCIT" value="cmdb_rel_ci" />
<property name="neebulaCIT" value="RELATION_BSS_MEMBER" />
<property name="cmdbService" ref="connectedTo_Service" />
- <property name="mappingRules">
- <map key-type="java.lang.String" value-type="java.lang.String">
<entry key="Type" value="5599a965c0a8010e00da3b58b113d70e'" />
<entry key="Parent" value="${src.id}" />
<entry key="Child" value="${target.id}" />
</map>
</property>
</bean>
- <bean id="AliasRule" class="java.util.ArrayList">
- <constructor-arg>
- <list value-type="com.doitwise.neebula.utils.Pair">
- <bean class="com.doitwise.neebula.utils.Pair">
<property name="first" value="Name" />
<property name="second" value="${label}+'@'+${host.Primary_host_name}" />
</bean>
</list>
</constructor-arg>
</bean>
- <bean id="BusinessServiceMatchingRule" class="java.util.ArrayList">
- <constructor-arg>
- <list value-type="com.doitwise.neebula.utils.Pair">
- <bean class="com.doitwise.neebula.utils.Pair">
<property name="first" value="Name" />
<property name="second" value="${label}" />
</bean>
</list>
</constructor-arg>
</bean>
- <bean id="ComputerSystemMatchingRule" class="java.util.ArrayList">
- <constructor-arg>
- <list value-type="com.doitwise.neebula.utils.Pair">
- <bean class="com.doitwise.neebula.utils.Pair">
<property name="first" value="Name" />
<property name="second" value="${host.Primary_host_name}" />
</bean>
- <bean class="com.doitwise.neebula.utils.Pair">
<property name="first" value="Name" />

```

```
<property name="second" value="${host.Primary_management_IP}" />
</bean>
- <bean class="com.doitwise.neebula.utils.Pair">
<property name="first" value="IpAddress" />
<property name="second" value="${host.Primary_management_IP}" />
</bean>
- <bean class="com.doitwise.neebula.utils.Pair">
<property name="first" value="serialNumber" />
<property name="second" value="${Serial_number}" />
</bean>
</list>
</constructor-arg>
</bean>
- <!--
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="discoverySource" value="Neebula" />
</map>
</constructor-arg>
</bean>
</beans>
```