INTEGRATION PACK FOR NAGIOS XI

For Microsoft System Center Orchestrator

User Guide

Version 1.4

Kelverion Integration Pack for Nagios XI

Published: March 2021

Feedback

Send suggestions and comments about this document to support@kelverion.com

Contents

Getting Started

The Integration Pack for Nagios XI is an add-on for System Center Orchestrator that enables you to integrate with Nagios XI functionality.

System Requirements

The Integration Pack for Nagios XI requires the following software to be installed and configured prior to implementing the integration. For more information about installing and configuring Orchestrator and Nagios XI, refer to the respective product documentation.

- Microsoft System Center Orchestrator *
- Microsoft .NET Framework 4.5.2
- Nagios XI 5.5.2, 5.8.2

* Please see Kelverion.com/orchestrator for the latest Orchestrator support information.

Important: The Integration Pack for Nagios XI requires the Nagios XI Event Log to be enabled. The Alerts and Log Entry activities will not return any records when the Nagios XI Event Log is disabled.

Important: If you are upgrading from Integration Pack for Nagios XI 1.2.x or earlier, then you must update your Nagios XI configuration options in Orchestrator. Please see the User Guide for details of new configuration changes.

Registering and Deploying the Integration Pack

After you download the integration pack file, you must register it with the Orchestrator management server and then deploy it to Runbook Servers and Runbook Designers. For more information about how to install integration packs, see the How to Install an Integration Pack.

To register the integration pack:

1. On the management server, copy the **.OIP** file for the integration pack to a local hard drive or network share.
2. Confirm that the file is not set to **Read Only** to prevent unregistering the integration pack later.
3. Start the **Deployment Manager**.
4. In the navigation pane of the Deployment Manager, expand **Orchestrator Management Server**, right-click **Integration Packs** to select **Register IP with the Orchestrator Management Server**. The **Integration Pack Registration Wizard** opens.
5. Click **Next**.
6. In the **Select Integration Packs or Hotfixes** dialog box, click **Add**.
7. Locate the **.OIP** file that you copied locally from step 1, click **Open** and then click **Next**.

8. In the **Completing the Integration Pack Wizard** dialog box, click **Finish**.
9. On the **End User Agreement** dialog box, read the Kelverion License Terms**,** and then click **Accept**.
10. The **Log Entries** pane displays a confirmation message when the integration pack is successfully registered.

To deploy the integration pack:

1. In the navigation pane of the **Deployment Manager**, right-click **Integration Packs**, click **Deploy IP to Runbook Server or Runbook Designer**.
2. Select the integration pack that you want to deploy, and then click **Next**.
3. Enter the name of the runbook server or computers with the Runbook Designer installed, on which you want to deploy the integration pack, click **Add**, and then click **Next**.
4. Continue to add additional runbook servers and computers running the Runbook Designer, on which you want to deploy the integration pack. Click **Next**.
5. In the **Installation Options** dialog box, configure the following settings.
6. To choose a time to deploy the integration pack, select the **Schedule installation** check box, and then select the time and date from the **Perform installation** list.
7. Click one of the following:
    a. **Stop all running runbooks before installing the integration pack** to stop all running runbooks before deploying the integration pack.
    b. **Install the Integration Packs without stopping the running Runbooks** to install the integration pack without stopping any running runbooks.
8. Click **Next**.
9. In the **Completing Integration Pack Deployment Wizard** dialog box, Click **Finish**.
10. When the integration pack is deployed, the **Log Entries** pane displays a confirmation message.

Licensing the Integration Pack

After you register and deploy the integration pack you must provide a valid Kelverion license before running any runbooks that contain activities from the integration pack

To deploy the integration pack license file:

1. Copy the .KAL license file to %PROGRAMFILES(X86)%\Kelverion Automation\Licenses
2. Repeat for each Orchestrator Runbook Server and Runbook Designer host system.

Configuring the Integration Pack

A connection establishes a reusable link between Orchestrator and a Nagios XI server. You can create as many connections as you require specifying links to multiple Nagios servers. You can also create multiple connections to the same server to allow for differences in security permissions for different user accounts.

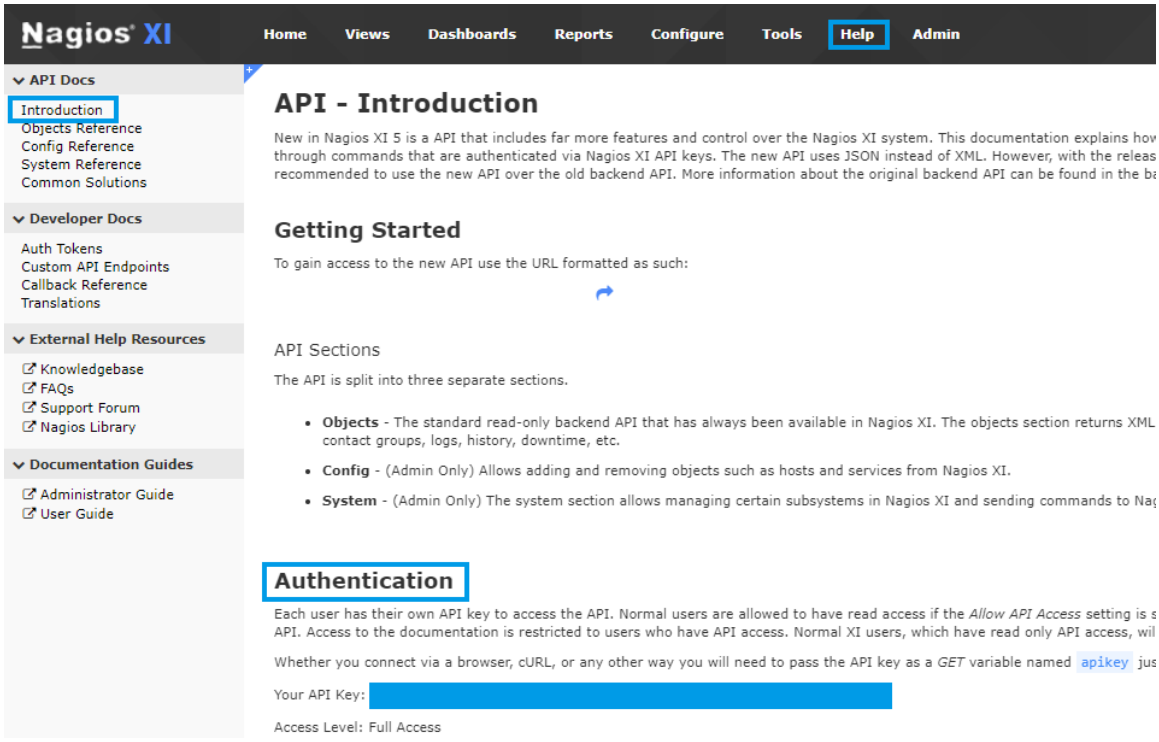
To set up a Nagios XI configuration:

1. In the Client, click the **Options** menu, and select *KA Nagios XI*. The **KA Nagios XI** dialog box appears.
2. On the **Configurations** tab, click **Add** to begin the configuration setup. The **Add Configuration** dialog box appears.
3. In the **Name** box, enter a name for the configuration. This could be the name of the Nagios server or a descriptive name to distinguish the type of configuration.
4. Click the ellipsis button (…) next to the **Type** box and select *Nagios XI.*
5. In the **Nagios XI Server URL** box, type the URL of the Nagios XI server. For example:
    - http://172.16.254.1 or
    - https://VM-NAGIOSXI-01.kelverion.com
6. In the **User Name** and **Password** boxes, type the credentials that the IP will use to connect to the Nagios XI server when running action type activities, for example *Acknowledge Problem, Schedule Downtime*, etc.
7. In the **Key** box enter the API key corresponding to the provided *User Name*. The IP will use the hey when running query type activities, for example *Get Host Stats, Monitor Alerts*, etc. See Obtaining the Nagios XI User Key section bellow, for details.
8. In the **Timeout** box enter the number of seconds the IP should wait before timing out when communicating with the Nagios server.
9. In the **Skip Certificate Validation** box, specify if you want the IP to perform server certificate validation or not. This applies only when connecting to the server over HTTPS. When set to **True**, the IP will not perform certificate validation, typically used in secure environments, when working with trusted servers and self-signed certificates. When set to **False**, the IP will validate the server certificate. The server must be configured with a valid certificate signed by a valid certificate authority and the specified Nagios XI server name must be listed on the certificate.
10. Add additional connections if applicable.
11. Click **OK** to close the configuration dialog box, and then click **Finish**.

Obtaining the Nagios XI User Key

The Nagios XI user key is required by the IP to invoke the Nagios XI REST API. Follow these steps to obtain the key:

1. Log into your Nagios XI web client console with the user whose key you want to find.
2. Click the **Help** link in the top menu.
3. Under API Docs on the left side, click on the **Introduction** link.
4. The key can be found in the **Authentication** section.
5. This is the key for the currently logged in user. You can copy and paste this in the **Key** property in the IP configuration settings.



Nagios XI Activities

This integration pack adds the KA Nagios XI category to the **Activities** pane in the Client. This category contains the following activities:

- Acknowledge Problem
- Get Alerts
- Get Host Status
- Get Hosts
- Get Log Entries
- Get Scheduled Downtime
- Get Service Status
- Get Services
- Get State History
- Monitor Alerts
- Monitor Host Status
- Monitor Log Entries
- Monitor Service Status
- Remove Acknowledgement
- Schedule Downtime

Common Configuration Instructions for All Activities

The following configuration instructions apply to all activities in this integration pack. Links to this section are included in the configuration instructions for each activity.

Activity Properties

Each activity has a set of required or optional properties that define the configuration of that activity. This includes how it connects to other activity or how the activity performs its actions. You can view or modify activity properties in the Orchestrator Client.

To configure the properties for an activity:

1. Double-click the activity. Alternatively, you can right-click the activity, and then click **Properties**.
2. To save your configuration entries, click **Finish**.

In the activity properties dialog box, several tabs along the left side provide access to general and specific settings for the activity. Although the number of available tabs for activity properties differs from activity to activity, all activities will have a **General** tab, a **Properties** tab and/or **Filters** tab, and a **Run Behavior** tab. Some activities may have additional tabs.

General Tab

This tab contains the **Name** and **Description** properties for the activity. By default, the **Name** of the activity is the same as its activity type, and the **Description** is blank. You can modify these properties to create more descriptive names or provide detailed descriptions of the actions of the activity.

Properties/Filters Tab

These tabs contain properties that are specific to the activity.

All activities in this integration pack have the **Configuration Name** property at the top of the **Properties** tab. This property is used to specify the connection to a Nagios XI server.

To configure the Configuration Name property:

1. Click the ellipsis **(…)** button next to the **Name** box, and then select the applicable connection name. Connections displayed in the list have been previously configured as described in Configuring the Nagios XI Connections.

Filter Behavior

The Monitor and Get activities use filters to determine the values that will invoke a runbook or retrieve activities. Property values of potential candidates are compared to the values of the filters to determine if they meet the criteria. When matching against values, you select one of the available methods of comparison. An option is provided to either match or not match the filter using each method. For example, the "Does not" version of a method causes records that do not match the filter to trigger the runbook. The Monitor activity will only trigger if all filters match and the Get activity will only return records that match all filters.

- **Equals**: the field of the record exactly matches the text or number specified in the filter.
- **Does not equal**: the field of the record does not exactly match the text or number specified in the filter.
- **Is less than**: the field of the record is less than the number specified in the filter.
- **Is less than or equal to**: the field of the record is less than or equal to the number specified in the filter.
- **Is greater than**: the field of the record is greater than the number specified in the filter.
- **Is greater than or equal to**: the field of the record is greater than or equal to the number specified in the filter.
- **Contains**: the filed of the record contains the text specified in the filter. The wildcard characters, '%' and '_' can be used to match multiple characters or a single character, respectively.
- **Does Not Contain**: the filed of the record does not contain the text specified in the filter. The wildcard characters, '%' and '_' can be used to match multiple characters or a single character, respectively.
- **Starts With**: the filed of the record starts with the text specified in the filter. The wildcard characters, '%' and '_' can be used to match multiple characters or a single character, respectively.
- **Ends With**: the filed of the record ends with the text specified in the filter. The wildcard characters, '%' and '_' can be used to match multiple characters or a single character, respectively.
- **Matches**: use wildcards to specify a pattern that the text must match. The two wildcard values are the percent (%) and the underscore (_). The percent will match any number of characters, while the underscore will only match a single character.
- **Does not match**: use wildcards to specify a pattern that the text does not match. The two wildcard values are the percent (%) and the underscore (_). The percent will match any number of characters, while the underscore will only match a single character.

Tip: *When using wildcard filters (Contains, Does Not Contain, Starts With, Ends With, Matches, Does Not Match), if the filter text value you are searching for contains the wildcard characters, '%' and '_', these characters can be escaped using backslash: '\%' and '_', respectively.*

Valid Special Characters In Filters

Due to limitations in the Nagios API, certain special characters have been restricted from being used in filter values. The following table lists the special characters which **can be used** in filter values:

Filter Operator	Valid Special Characters	Wildcards	Escaped
Equals	**~ ` ! @ $ ^ * ( ) . [ ] { } | . / ? # + % _ \ :**		
Does Not Equal	**~ ` ! @ $ ^ * ( ) . [ ] { } | . / ? # + % _ **		
Contains Does Not Contain Starts With Ends With Matches Does Not Match	**~ ` ! @ $ ^ * ( ) . [ ] { } | . / ? # +**	**% _ **	**\%** **_** ****

Tip: *As a safe practice, we recommend restricting characters in filter values to alpha-numeric set.*

Run Behavior Tab

This tab contains the properties that determine how the activity handles multi-value published data and what notifications will be sent if the activity fails or runs for an excessive period of time.

Multi-Value Published Data Behavior

The Get activities retrieve information from another activity or outside source, and can return one or more values in the published data. For example, when you use the Get Collection Member activity, the data output from that activity might be a list of computers that belong to the specified collection.

By default, the data from the Get activity will be passed on as multiple individual outputs. This invokes the next activity as many times as there are items in the output. Alternatively, you can provide a single output for the activity by enabling the **Flatten** option. When you enable this option, you also choose a formatting option:

- **Separate with line breaks**. Each item is on a new line. This format is useful for creating human-readable text files for the output.
- **Separate with _** . Each item is separated by one or more characters of your choice.
- **Use CSV format**. All items are in CSV (comma-separated value) format. This format is useful for importing data into spreadsheets or other applications.

The activity will produce a new set of data every time it runs. The **Flatten** feature does not flatten data across multiple instances of the same activity.

Event Notifications

Some activities are expected to take a limited amount of time to complete. If they do not complete within that time they may be stalled or there may be another issue preventing them from completing. You can define the number of seconds to wait for completion of the action. After this period a platform event will be sent and the issue will be reported. You can also choose whether to generate a platform event if the activity returns a failure.

To be notified when the activity takes longer than a specified time to run or fails to run:

1. In the **Event Notifications** box, enter the **number of seconds** of run time before a notification is generated.
2. Select **Report if activity fails to run** to generate run failure notifications.

For more information about Orchestrator events, see the "Event Notifications " topics in the Runbook Properties (https://technet.microsoft.com/en-us/library/hh489610.aspx#Event Notifications).

Published Data

Published data is the foundation of a working runbook. It is the data produced as a result of the actions of an activity. This data is published to an internal data bus that is unique for each runbook. Subsequent activities in the runbook can subscribe to this data and use it in their configuration. Link conditions also use this information to add decision-making capabilities to runbooks.

An activity can only subscribe to data from the activities that are linked before it in the runbook. You can use published data to automatically populate the property values needed by activities.

To use published data:

1. Right-click the property value box, click **Subscribe**, and then click **Published Data**.
2. Click the **Activity** drop-down box and select the activity from which you want to obtain the data.
3. To view additional data elements common to all activities, select **Show Common Published Data**.
4. Click the published data element that you want to use, and then click **OK**.

For a list of the data elements published by each activity, see the Published Data tables in the activity topic. For information about the common published data items, see the Published Data (http://technet.microsoft.com/en-us/library/hh403821.aspx).

Nagios XI Common Published Data

The following table describes the activity-specific data that is published by all of the activities in the Integration Pack for Nagios XI.

Nagios XI Server URL	URL of the Nagios XI server. For example: 1. http://172.16.254.1 2. https://VM-NAGIOSXI-01.kelverion.com
User Name	User Name which the IP uses to connect to the Nagios XI server.

Acknowledge Problem Activity

The **Acknowledge Problem** activity is used in a runbook to acknowledge host and service problems.

Required Properties

You must configure the following properties.

Author Name	Specifies user acknowledging the problem. Default value is *User Name* specified in the IP activity configuration.
Comment	Acknowledgement comment.
Host Name	Name of host with the problem (or host with a service which has a problem).
Is Sticky	Specifies if problem acknowledgement is sticky or not.
Object Type	Specifies the type of object whose problem is being acknowledged. Options include HOST and SERVICE.
Persistent Comment	Specifies whether comment should be persisted or not.
Send Notification	Specifies if a notification should be sent.
Service	Service with the problem
Wait to Complete	Specifies whether the activity should wait for the problem to be acknowledged, before completing. Use *Wait Timeout* to specify a timeout period. If configured to wait and *Wait Timeout* is not specified the activity waits until the problem has been acknowledged.

Optional Properties

You can configure the following properties, as required.

Wait Timeout (sec)	Specifies how long the activity should wait for the problem to be acknowledged, before completing. Use this property when *Wait To Complete* is set to *True*.

Published Data

This activity publishes the following activity-specific items.

Host Name	Host whose problem is being acknowledged.
Object Type	Type of object whose problem acknowledgement is being removed. Values include Host and Service.
Problem Acknowledged	When *Wait To Complete* is set to *True*, this indicates whether the problem was acknowledged at the time when the activity completed.
Service	Service whose problem is being acknowledged, when acknowledging a service problem.

Get Alerts Activity

The **Get Alerts** activity is used in a runbook to retrieve and filter host and service alerts.

Important: This activity requires the Nagios XI Event Log to be enabled. If the Event Log is not enabled, the activity will return zero records.

Required Properties

You must configure the following properties.

Tip: Use the Start Time and End Time properties to limit the volume of data returned by Nagios server.

Start Time	Specifies start time of the period for which alerts are to be retrieved.
End Time	Specifies end time of the period for which alerts are to be retrieved.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which alert records to retrieve and publish to the Orchestrator data bus.

Tip: It is recommended to filter first by Alert Details and Alert Type and then narrow down the result set further by using the remaining filters.

Alert Details	Filter by Alert Details.
Alert Text	Filter by Alert Text.
Alert Type	Filter by Alert Type. See remarks for details.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Service Description	Filter by Service Description.
State Type	Filter by State Type. Options include HARD and SOFT.

Published Data

This activity publishes the following activity-specific items.

Alert Count	Number of alert records returned.
Alert Details	Alert detail information.
Alert Time	Time of the alert.
Alert Type	Specifies the alert type. See remarks for details.
Host Name	Name of host that generated the alert.
Instance ID	Specifies alert identifier.
Service Description	Service that generated the alert.

State Type	Type of state. Possible values include HARD and SOFT.SOFT

Remarks

When configuring the **Alert Type** filter or using the **Alert Type** published data item, the following values are supported:

- HOST_UP
- HOST_DOWN
- HOST_UNREACHABLE
- SERVICE_OK
- SERVICE_UNKNOWN
- SERVICE_WARNING
- SERVICE_CRITICAL

Get Host Status Activity

The **Get Host Status** activity is used in a runbook to retrieve and filter Nagios host status information.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which host status record to retrieve and publish to the Orchestrator data bus.

Active Checks Enabled	Filter by Active Checks Enabled value.
Check Command	Filter by Check Command value.
Current Check Attempt	Current check attempt.
Current State	Filter by Current State. Options include UP, DOWN and UNREACHABLE.
Event Handler Enabled	Filter by Event Handler Enabled value.
Flap Detection Enabled	Filter by Flap Detection Enabled.
Host Address	Filter by Host Address value.
Host Alias	Filter by Host Alias.
Host Display Name	Filter by Host Display Name.
Host ID	Filter by Host ID.
Host Name	Filter by Host Name.
Host Status ID	Filter by Host Status ID.
Instance ID	Filter by Instance ID.
Is Flapping	Filter by Is Flapping value.
Is Pending	Filter by Is Pending value.
Last State Change	Filter by Last State Change value.
Notifications Enabled	Filter by Notifications Enabled value.
Passive Checks Enabled	Filter by Passive Checks Enabled value.
Problem Acknowledged	Filter by Problem Acknowledged value.
State Type	Filter by State Type value. Options include HARD and SOFT.
Status Update Time	Filter by Status Update Time value.

Published Data

This activity published the following activity-specific data.

Acknowledgement Type	Acknowledgement type. Possible values include NONE, NORMAL and STICY.
Active Checks Enabled	Specifies if active checks are enabled or not.
Check Command	Check command.
Check Time Period ID	Check Time Period ID
Check Type	Type of check performed. Possible values include ACTIVE, PASSIVE, PARENT, FILE and OTHER.
Current Check Attempt	Current check attempt.
Current Notification Number	Current notification number
Current State	Current host state. Possible values include UP, DOWN and UNREACHABLE.
Event Handler	Event handler.
Event Handler Enabled	Specifies if event handler is enabled or not.
Execution Time (sec)	Check execution time in seconds.
Flap Detection Enabled	Specifies if flap detection is enabled or not.
Has Been Checked	Specifies if host has been checked or not.
Host Address	Host IP address.
Host Alias	Host alias.
Host Display Name	Host display.
Host ID	Host identifier.
Host Name	Host name.
Host Status Count	Number of records returned by the activity
Host Status ID	Host status identifier.
Instance ID	Host status instance identifier.
Is Flapping	Specifies if flapping (state is changing too frequently) or not.
Is Pending	Specifies if status is pending or not.
Last Check	Date and time when last check was performed.
Last Hard State	Last hard state value.
Last Hard State Change	Last time when the hard state changed.
Last Notification	Time when last notification was sent.
Last State Change	Last time when the state changed.
Last Time Down	Last time when the host was down.

Last Time Unreachable	Last time when the host was unreachable.
Last Time Up	Last time when the host was up.
Latency (sec)	Check latency in seconds.
Max Check Attempts	Maximum number of check attempts.
Modified Host Attributes	Bitmask value indicating which attributes have changed. See the remarks section for details.
Next Check	Date and time when next check will be performed.
Next Notification	Date and time when next notification will be performed.
Normal Check Interval (min)	Number of minutes between checks.
Notifications Enabled	Specifies if notifications are enabled or not.
Obsess Over Host	Specifies if "obsessing" over host checks is enabled or not.
Passive Checks Enabled	Specifies if passive checks are enabled or not.
Percent State Change	Specifies the percent state change value.
Performance Data	Performance data.
Problem Acknowledged	Specifies if problem has been acknowledged or not.
Process Performance Data	Specifies if performance data should be processed or not.
Retry Check Interval (min)	Number of minutes between retires.
Scheduled Downtime Depth	Scheduled downtime depth.
Should Be Scheduled	Should be scheduled.
State Type	Specifies state type.
Status Text	Status text description.
Status Text Long	Long status text description.
Status Update Time	Date and time when status was updated.

Remarks

The numeric value that is published for the **Modified Host Attributes** data item is a bitmask, in which each bit in the number has the following meaning.

Binary Value	Decimal Value	Meaning
0000 0000 0000 0000 0000	0	NONE
0000 0000 0000 0000 0001	1	NOTIFICATIONS ENABLED
0000 0000 0000 0000 0010	2	ACTIVE CHECKS ENABLED
0000 0000 0000 0000 0100	4	PASSIVE CHECKS ENABLED

0000 0000 0000 0000 1000	8	EVENT HANDLER ENABLED
0000 0000 0000 0001 0000	16	FLAP DETECTION ENABLED
0000 0000 0000 0010 0000	32	FAILURE PREDICTION ENABLED
0000 0000 0000 0100 0000	64	PERFORMANCE DATA ENABLED
0000 0000 0000 1000 0000	128	OBSESSIVE HANDLER ENABLED
0000 0000 0001 0000 0000	256	EVENT HANDLER ENABLED
0000 0000 0010 0000 0000	512	CHECK COMMAND
0000 0000 0100 0000 0000	1024	NORMAL CHECK INTERVAL
0000 0000 1000 0000 0000	2048	RETRY CHECK INTERVAL
0000 0001 0000 0000 0000	4096	MAX CHECK ATTEMPTS
0000 0010 0000 0000 0000	8192	FRESHNES CHECKS ENABLED
0000 0100 0000 0000 0000	16384	CHECK TIMEPERIOD
0000 1000 0000 0000 0000	32768	CUSTOM VARIABLE
0001 0000 0000 0000 0000	65536	NOTIFICATION TIMEPERIOD

Get Hosts Activity

The **Get Hosts** activity is used in a runbook to retrieve and filter Nagios hosts.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which host records to retrieve and publish to the Orchestrator data bus.

Host Address	Filter by Host Address.
Host Alias	Filter by Host Alias.
Host Display Name	Filter by Host Display Name.
Host ID	Filter by Host ID.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Is Active	Filter by Is Active value.

Published Data

This activity publishes the following activity-specific items.

Active Checks Enabled	Specifies if active checks are enabled.
Check Interval (min)	Number of minutes between checks.
First Notification Delay (min)	Number of minutes to delay the first notification by.
Host Address	Host IP address.
Host Alias	Host alias.
Host Count	Number of records returned by the activity
Host Display Name	Host display name.
Host ID	Unique host identifier.
Host Name	Host name.
Instance ID	Host instance identifier.
Is Active	Specifies if host is active or not.
Max Check Attempts	Maximum number of check attempts.
Notes	Host notes.
Notification Interval	Number of minutes between notifications.
Notifications Enabled	Specifies if notifications are enabled.
Passive Checks Enabled	Specifies if passive checks are enabled.
Retry Interval (min)	Number of minutes between retires.

Get Log Entries Activity

The **Get Log Entries** activity is used in a runbook to retrieve and filter log entries from your Nagios XI system.

Important: This activity requires the Nagios XI Event Log to be enabled. If the Event Log is not enabled, the activity will return zero records.

Required Properties

You must configure the following properties.

Tip: Use the Start Time and End Time properties to limit the volume of data returned by Nagios server.

Start Time	Specifies start time of the period for which log entries are to be retrieved.
End Time	Specifies end time of the period for which log entries are to be retrieved.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which log entry records to retrieve and publish to the Orchestrator data bus.

Entry Details	Filter by Log Entry Details. See the remarks section for details.
Entry Type	Filter by log entry type.
Instance ID	Filter by Instance ID.

Published Data

This activity publishes the following activity-specific items.

Log Entry Count	Number of log entry records returned.
Entry Details	Log entry detail information.
Entry Time	Time of the log entry.
Entry Type	Specifies the log entry type. See the remarks section for details.
Instance ID	Specifies log entry identifier.

Remarks

When configuring the **Entry Type** filter or using the **Entry Type** published data item, the following values are supported.

- CONFIG_ERROR
- CONFIG_WARNING
- EVENT_HANDLER
- EXTERNAL_COMMAND
- HOST_DOWN
- HOST_NOTIFICATION
- HOST_UNREACHABLE
- HOST_UP

- INFO_MESSAGE
- NOTIFICATION
- PASSIVE_CHECK
- PROCESS_INFO
- RUNTIME_ERROR
- RUNTIME_WARNING
- SERVICE_CRITICAL
- SERVICE_NOTIFICATION
- SERVICE_OK
- SERVICE_UNKNOWN
- SERVICE_WARNING
- VERIFICATION_ERROR
- VERIFICATION_WARNING

Get Scheduled Downtime Activity

The **Get Scheduled Downtime** activity is used in a runbook to retrieve and filter host and service scheduled downtime information.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which scheduled downtime records to retrieve and publish to the Orchestrator data bus.

Actual Start Time	Filter by Actual Start Time.
Actual Start Time (microsec)	Filter by Actual Start Time microsecond component.
Author Name	Filter by Author Name.
Comment	Filter by Comment.
Downtime ID	Filter by Downtime ID.
Downtime Type	Filter by Downtime Type. Options include FIXED and FLEXIBLE.
Duration (sec)	Filter by Duration.
Entry Time	Filter by Entry Time.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Object ID	Filter by Object ID.
Object Type	Filter by Object Type. Options include HOST and SERVICE.
Scheduled End Time	Filter by Scheduled End Time.
Scheduled Start Time	Filter by Scheduled Start Time.
Service Description	Filter by Service.
Triggered By	Filter by Triggered By value.
Was Started	Filter by Was Started value.

Published Data

This activity publishes the following activity-specific items.

Actual Start Time	Actual start time for the downtime.
Actual Start Time (microsec)	Microsecond component for the Actual Start Time.
Author Name	User who scheduled the downtime.
Comment	Scheduled downtime comment.
Downtime ID	Downtime unique identifier.
Downtime Type	Type of downtime. Possible values include FIXED and FLEXIBLE**.**
Duration (sec)	Downtime duration.
Entry Time	Downtime entry time.
Host Name	Host targeted by downtime.
Instance ID	Downtime instance identifier.
Object ID	Object unique identifier.
Object Type	Type of object targeted by the downtime. Possible values include HOST and SERVICE.
Scheduled End Time	Scheduled end time of the downtime.
Scheduled Start Time	Scheduled start time of the downtime.
Service Description	Service targeted by the downtime when **Object Type** is Service.
Triggered By	Identifier of another scheduled downtime record which triggers this downtime.
Was Started	Specifies whether downtime period started or not.

Get Service Status Activity

The **Get Service Status** activity is used in a runbook to retrieve and filter Nagios service status information.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which service status records to retrieve and publish to the Orchestrator data bus.

Active Checks Enabled	Filter by Active Checks Enabled value.
Check Command	Filter by Check Command value.
Current Check Attempt	Current check attempt.
Current State	Filter by Current State. Options include OK, WARNING, CRITICAL and UNKNOWN.
Event Handler Enabled	Filter by Event Handler Enabled value.
Flap Detection Enabled	Filter by Flap Detection Enabled.
Has Been Checked	Filter by Has Been Checked value.
Host Address	Filter by Host Address value.
Host Display Name	Filter by Host Display Name.
Host ID	Filter by Host ID.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Is Flapping	Filter by Is Flapping value.
Is Pending	Filter by Is Pending value.
Last State Change	Filter by Last State Change value.
Notifications Enabled	Filter by Notifications Enabled value.
Passive Checks Enabled	Filter by Passive Checks Enabled value.
Problem Acknowledged	Filter by Problem Acknowledged value.
Service ID	Filter by Status ID.
Service Name	Filter by Service Name.
Service Status ID	Filter by Service Status ID.
State Type	Filter by State Type value.
Status Update Time	Filter by Status Update Time value.

Published Data

This activity publishes the following activity-specific items.

Acknowledgement Type	Acknowledgement Type. Possible values include NONE, NORMAL and STICKY.
Active Checks Enabled	Specifies if active checks are enabled or not.
Check Command	Check command.
Check Time Period ID	Check Time Period ID
Check Type	Type of check performed. Possible values include ACTIVE, PASSIVE, PARENT, FILE and OTHER.
Current Check Attempt	Current check attempt.
Current Notification Number	Current notification number
Current State	Current service state. Possible values include OK, WARNING, CRITICAL and UNKNOWN.
Event Handler	Event handler.
Event Handler Enabled	Specifies if event handler is enabled or not.
Execution Time (sec)	Check execution time in seconds.
Flap Detection Enabled	Specifies if flap detection is enabled or not.
Has Been Checked	Specifies if service has been checked or not.
Host Address	Host IP address.
Host Display Name	Host display.
Host ID	Host identifier.
Host Name	Host name.
Instance ID	Service status instance identifier.
Is Flapping	Specifies if flapping (state is changing too frequently) or not.
Is Pending	Specifies if status is pending or not.
Last Check	Date and time when last check was performed.
Last Hard State	Last hard state value. Possible values include OK, WARNING, CRITICAL and UNKNOWN.
Last Hard State Change	Last time when the hard state changed.
Last Notification	Time when last notification was sent.
Last State Change	Last time when the state changed.
Last Time Critical	Last time when the service status was Critical.
Last Time OK	Last time when the service status was OK.
Last Time Unknown	Last time when the service status was Unknown.

Last Time Warning	Last time when the service status was Warning.
Latency (sec)	Check latency in seconds.
Max Check Attempts	Maximum number of check attempts.
Modified Service Attributes	Bitmask value indicating which attributes have changed. See the remarks section below for details.
Next Check	Date and time when next check will be performed.
Next Notification	Date and time when next notification will be performed.
Normal Check Interval (min)	Number of minutes between checks.
Notifications Enabled	Specifies if notifications are enabled or not.
Obsess Over Service	Specifies if "obsessing" over service checks is enabled or not.
Passive Checks Enabled	Specifies if passive checks are enabled or not.
Percent State Change	Specifies the percent state change value.
Performance Data	Performance data.
Problem Acknowledged	Specifies if problem has been acknowledged or not.
Process Performance Data	Specifies if performance data should be processed or not.
Retry Check Interval (min)	Number of minutes between retires.
Scheduled Downtime Depth	Scheduled downtime depth.
Service ID	Service identifier.
Service Name	Service name.
Service Status Count	Number of records returned by the activity
Service Status ID	Service status identifier.
Should Be Scheduled	Should be scheduled.
State Type	Specifies state type. Possible values include HARD and SOFT.
Status Text	Status text description.
Status Text Long	Long status text description.
Status Update Time	Date and time when status was updated.

Remarks

The numeric value that is published for the **Modified Service Attributes** data item is a bitmask, in which each bit in the number has the following meaning.

Binary Value	Decimal Value	Meaning
0000 0000 0000 0000 0000	0	NONE
0000 0000 0000 0000 0001	1	NOTIFICATIONS ENABLED
0000 0000 0000 0000 0010	2	ACTIVE CHECKS ENABLED
0000 0000 0000 0000 0100	4	PASSIVE CHECKS ENABLED
0000 0000 0000 0000 1000	8	EVENT HANDLER ENABLED
0000 0000 0000 0001 0000	16	FLAP DETECTION ENABLED
0000 0000 0000 0010 0000	32	FAILURE PREDICTION ENABLED
0000 0000 0000 0100 0000	64	PERFORMANCE DATA ENABLED
0000 0000 0000 1000 0000	128	OBSESSIVE HANDLER ENABLED
0000 0000 0001 0000 0000	256	EVENT HANDLER ENABLED
0000 0000 0010 0000 0000	512	CHECK COMMAND
0000 0000 0100 0000 0000	1024	NORMAL CHECK INTERVAL
0000 0000 1000 0000 0000	2048	RETRY CHECK INTERVAL
0000 0001 0000 0000 0000	4096	MAX CHECK ATTEMPTS
0000 0010 0000 0000 0000	8192	FRESHNES CHECKS ENABLED
0000 0100 0000 0000 0000	16384	CHECK TIMEPERIOD
0000 1000 0000 0000 0000	32768	CUSTOM VARIABLE
0001 0000 0000 0000 0000	65536	NOTIFICATION TIMEPERIOD

Get Services Activity

The **Get Services** activity is used in a runbook to retrieve and filter Nagios services.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which service records to retrieve and publish to the Orchestrator data bus.

Display Name	Filter by Display Name.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Is Active	Filter by Is Active value.
Service Description	Filter by Service description.
Service ID	Filter by Service ID.

Published Data

This activity publishes the following activity-specific items.

Active Checks Enabled	Specifies if active checks are enabled.
Check Interval (min)	Number of minutes between checks.
First Notification Delay (min)	Number of minutes to delay the first notification by.
Host Name	Host where service is running.
Instance ID	Service instance identifier.
Is Active	Specifies if service is active or not.
Max Check Attempts	Maximum number of check attempts.
Notes	Service notes.
Notification Interval	Number of minutes between notifications.
Notifications Enabled	Specifies if notifications are enabled.
Passive Checks Enabled	Specifies if passive checks are enabled.
Retry Interval (min)	Number of minutes between retires.
Service Count	Number of records returned by the activity
Service Description	Service description
Service Display Name	Service display name.
Service ID	Unique service identifier.

Get State History Activity

The **Get State History** activity is used in a runbook to retrieve and filter host and service state history information.

Required Properties

You must configure the following properties.

Tip: Use the Start Time and End Time properties to limit the volume of data returned by Nagios server.

Start Time	Specifies start time of the period for which state history is to be retrieved.
End Time	Specifies end time of the period for which state history is to be retrieved.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which state history records to retrieve and publish to the Orchestrator data bus.

Current Check Attempt	Filter by Current Check Attempt value.
Host Name	Filter by Host Name.
Information	Filter by state Information.
Instance ID	Filter by Instance ID.
Last Hard State	Filter by Last Hard State value.
Last State	Filter by Last State value. See remarks for details.
Max Check Attempts	Filter by Max Check Attempts.
Object ID	Filter by Object ID.
Object Type	Filter by Object Type. Options include HOST and SERVICE.
Service Description	Filter by Service Description.
State	Filter by State value. See remarks for details.
State Change	Filter by State Change.
State Time	Filter by State Time.
State Type	Filter by State Type. Options include HARD and SOFT.

Published Data

This activity publishes the following activity-specific items.

Current Check Attempt	Current check attempt.
Host Name	Host name.
Information	State information.
Instance ID	State history instance identifier.
Last Hard State	Last hard state value for host or service.
Last State	Last state value for host or service. See the remarks section for details.
Max Check Attempts	Maximum number of check attempts.
Object ID	Host or service object identifier.
Object Type	Object type. Possible values include HOST and SERVICE.
Service Description	Service description, for service records.
State	State value for host or service. See the remarks section for details.
State Change	State change.
State Entry Count	Number of state history records returned.
State Time	Time when state was recorded.
State Type	Type of state. Possible values include HARD and SOFT.

Remarks

Nagios uses state information to indicate:

- When host state is UP, or service state is OK.
- When host state is DOWN, or service state is WARNING.
- When host state is UNREACHABLE, or service state is CRITICAL.

When configuring filters that represent state, the following values are supported. Similarly, when using published data items that represent state, the following values may include the following.

- NULL
- HOST_UP
- HOST_DOWN
- HOST_UNREACHABLE
- SERVICE_OK
- SERVICE_WARNING
- SERVICE_CRITICAL
- SERVICE_UNKNOWN

Monitor Alerts Activity

The **Monitor Alerts** activity is used in a runbook to monitor Nagios host and service alerts.

Important: This activity requires the Nagios XI Event Log to be enabled. If the Event Log is not enabled, the activity will return zero records.

Required Properties

You must configure the following properties.

Monitor Interval (sec)	Specifies how often, in seconds, the monitor checks the Nagios server for new alerts. Minimum value is 15 seconds.
Lag Tolerance (minutes)	Specifies, in minutes, how far into the past from the most recent triggered event, the activity should continue to monitor for new events that have yet to be reported.

Optional Properties

You can configure the following properties, as required.

Host Group Name	Specifies a host group to be monitored. The monitor will only trigger on host alerts for hosts which are part of this host group. The monitor will only trigger on service alerts for services belonging to hosts which are part of this host group.
Service Group Name	Specifies a service group to be monitored. The monitor will only trigger on service alerts for services which are part of this service group.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which alert records will trigger the monitor and be published to the Orchestrator data bus.

Tip: It is recommended to filter first by Alert Details and Alert Type and then narrow down the result set further by using the remaining filters.

Alert Details	Filter by Alert Details.
Alert Text	Filter by Alert Text.
Alert Time	Filter by Alert Time.
Alert Type	Filter by Alert Type. See remarks for details.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Service Description	Filter by Service Description.
State Type	Filter by State Type. Options include HARD and SOFT.

Published Data

This activity publishes the following activity-specific items.

Alert Count	Number of alert records returned.
Alert Details	Alert detail information.
Alert Time	Time of the alert.
Alert Type	Specifies the alert type. See the remarks section for details.
Host Name	Name of host that generated the alert.
Instance ID	Specifies alert identifier.
Service Description	Service that generated the alert.
State Type	Type of state. Possible values include HARD and SOFT.

Remarks

When configuring the **Alert Type** filter the following options are supported. Similarly, when using the **Alert Type** published data item, the following values may be included.

- HOST_UP
- HOST_DOWN
- HOST_UNREACHABLE
- SERVICE_OK
- SERVICE_UNKNOWN
- SERVICE_WARNING
- SERVICE_CRITICAL

Monitor Host Status Activity

The **Monitor Host Status** activity is used in a runbook to detect status changes for Nagios hosts.

Tip: By default, the monitor reports both hard and soft state changes, use the **State Type** filter to trigger for specific state type.

Note: By default, when the host is in a soft state, the monitor triggers for each host check. Use the **Current Check Attempt** filter, according to your *Max Check Attempts* configuration in Nagios server, to filter out extra triggers.

Required Properties

You must configure the following properties.

Monitor Interval (sec)	Specifies how often, in seconds, the monitor checks the Nagios server for status changes. Minimum value is 15 seconds.
Lag Tolerance (minutes)	Specifies, in minutes, how far into the past from the most recent triggered event, the activity should continue to monitor for new events that have yet to be reported.

Optional Properties

You can configure the following properties, as required.

Host Group Name	Specifies a host group to be monitored. The monitor will only trigger on host status changes for hosts which are part of this host group.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which host status records will trigger the monitor and be published to the Orchestrator data bus.

Active Checks Enabled	Filter by Active Checks Enabled value.
Check Command	Filter by Check Command value.
Current Check Attempt	Filter by Current Check Attempt.
Current State	Filter by Current State. Options included UP, DOWN and UNREACHABLE.
Event Handler Enabled	Filter by Event Handler Enabled value.
Flap Detection Enabled	Filter by Flap Detection Enabled.
Host Address	Filter by Host Address value.
Host Alias	Filter by Host Alias.
Host Display Name	Filter by Host Display Name.
Host ID	Filter by Host ID.

Host Name	Filter by Host Name.
Host Status ID	Filter by Host Status ID.
Instance ID	Filter by Instance ID.
Is Flapping	Filter by Is Flapping value.
Is Pending	Filter by Is Pending value.
Notifications Enabled	Filter by Notifications Enabled value.
Passive Checks Enabled	Filter by Passive Checks Enabled value.
Problem Acknowledged	Filter by Problem Acknowledged value.
State Type	Filter by State Type value. Options include HARD and SOFT.
Status Update Time	Filter by Status Update Time value.

Published Data

This activity publishes the following activity-specific items.

Acknowledgement Type	Acknowledgement type. Possible values include NONE, NORMAL and STICKY.
Active Checks Enabled	Specifies if active checks are enabled or not.
Check Command	Check command.
Check Time Period ID	Check Time Period ID
Check Type	Type of check performed. Possible values include ACTIVE, PASSIVE, PARENT, FILE and OTHER.
Current Check Attempt	Current check attempt.
Current Notification Number	Current notification number
Current State	Current host state. Possible values include UP, DOWN and UNREACHABLE.
Event Handler	Event handler.
Event Handler Enabled	Specifies if event handler is enabled or not.
Execution Time (sec)	Check execution time in seconds.
Flap Detection Enabled	Specifies if flap detection is enabled or not.
Host Address	Host IP address.
Host Alias	Host alias.
Host Display Name	Host display name.
Host ID	Host identifier.
Host Name	Host name.
Host Status Count	Number of records returned by the activity

Host Status ID	Host status identifier.
Instance ID	Host status instance identifier.
Is Flapping	Specifies if flapping (state is changing too frequently) or not.
Is Pending	Specifies if status is pending or not.
Last Check	Date and time when last check was performed.
Last Hard State	Last hard state value. Possible values include UP, DOWN and UNREACHABLE.
Last Hard State Change	Last time when the hard state changed.
Last Notification	Time when last notification was sent.
Last State Change	Last time when the state changed.
Last Time Down	Last time when the host was down.
Last Time Unreachable	Last time when the host was unreachable.
Last Time Up	Last time when the host was up.
Latency (sec)	Check latency in seconds.
Max Check Attempts	Maximum number of check attempts.
Modified Host Attributes	Bitmask value indicating which attributes have changed.
Next Check	Date and time when next check will be performed.
Next Notification	Date and time when next notification will be performed.
Normal Check Interval (min)	Number of minutes between checks.
Notifications Enabled	Specifies if notifications are enabled or not.
Obsess Over Host	Specifies if “obsessing” over host checks is enabled or not.
Passive Checks Enabled	Specifies if passive checks are enabled or not.
Percent State Change	Specifies the percent state change value.
Performance Data	Performance data.
Problem Acknowledged	Specifies if problem has been acknowledged or not.
Process Performance Data	Specifies if performance data should be processed or not.
Retry Check Interval (min)	Number of minutes between retires.
Scheduled Downtime Depth	Scheduled downtime depth.
Should Be Scheduled	Should be scheduled.
State Type	Specifies state type. Possible values include HARD and SOFT.
Status Text	Status text description.
Status Text Long	Long status text description.

Status Update Time	Date and time when status was updated.

Remarks

The numeric value that is published for the **Modified Host Attributes** data item is a bitmask, in which each bit in the number has the following meaning.

Binary Value	Decimal Value	Meaning
0000 0000 0000 0000 0000	0	NONE
0000 0000 0000 0000 0001	1	NOTIFICATIONS ENABLED
0000 0000 0000 0000 0010	2	ACTIVE CHECKS ENABLED
0000 0000 0000 0000 0100	4	PASSIVE CHECKS ENABLED
0000 0000 0000 0000 1000	8	EVENT HANDLER ENABLED
0000 0000 0000 0001 0000	16	FLAP DETECTION ENABLED
0000 0000 0000 0010 0000	32	FAILURE PREDICTION ENABLED
0000 0000 0000 0100 0000	64	PERFORMANCE DATA ENABLED
0000 0000 0000 1000 0000	128	OBSESSIVE HANDLER ENABLED
0000 0000 0001 0000 0000	256	EVENT HANDLER ENABLED
0000 0000 0010 0000 0000	512	CHECK COMMAND
0000 0000 0100 0000 0000	1024	NORMAL CHECK INTERVAL
0000 0000 1000 0000 0000	2048	RETRY CHECK INTERVAL
0000 0001 0000 0000 0000	4096	MAX CHECK ATTEMPTS
0000 0010 0000 0000 0000	8192	FRESHNES CHECKS ENABLED
0000 0100 0000 0000 0000	16384	CHECK TIMEPERIOD
0000 1000 0000 0000 0000	32768	CUSTOM VARIABLE
0001 0000 0000 0000 0000	65536	NOTIFICATION TIMEPERIOD

Monitor Log Entries Activity

The Get Log Entries activity is used in a runbook to monitor log entries from your Nagios XI system.

Important: This activity requires the Nagios XI Event Log to be enabled. If the Event Log is not enabled, the activity will return zero records.

Required Properties

You must configure the following properties.

Monitor Interval (sec)	Specifies how often, in seconds, the monitor checks the Nagios server for new log entries. Minimum value is 15 seconds.
Lag Tolerance (minutes)	Specifies, in minutes, how far into the past from the most recent triggered event, the activity should continue to monitor for new events that have yet to be reported.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which log entry records will trigger the monitor and be published to the Orchestrator data bus.

Entry Details	Filter by *Log Entry Details.*
Entry Type	Filter by log entry type. See remarks for details.
Instance ID	Filter by Instance ID.

Published Data

This activity publishes the following activity-specific items.

Log Entry Count	Number of log entry records returned.
Entry Details	Log entry detail information.
Entry Time	Time of the log entry.
Entry Type	Specifies the log entry type. See remarks for details.
Instance ID	Specifies log entry identifier.

Remarks

When configuring the **Entry Type** filter or interpreting the **Entry Type** published date item, the following values are available.

- CONFIG_ERROR
- CONFIG_WARNING
- EVENT_HANDLER
- EXTERNAL_COMMAND
- HOST_DOWN
- HOST_NOTIFICATION
- HOST_UNREACHABLE
- HOST_UP
- INFO_MESSAGE
- NOTIFICATION

- PASSIVE_CHECK
- PROCESS_INFO
- RUNTIME_ERROR
- RUNTIME_WARNING
- SERVICE_CRITICAL
- SERVICE_NOTIFICATION
- SERVICE_OK
- SERVICE_UNKNOWN
- SERVICE_WARNING
- VERIFICATION_ERROR

Monitor Service Status Activity

The **Monitor Service Status** activity is used in a runbook to detect status changes for Nagios services. The following tables list the inputs, published data and filters for this activity.

Tip: By default, the monitor reports both hard and soft state changes, use the *State Type* filter to trigger for specific state type.

Tip: By default, when the service is in a soft state, the monitor triggers for each service check. Use the *Current Check Attempt* filter, according to your *Max Check Attempts* configuration in Nagios server, to filter out extra triggers.

Required Properties

You must configure the following properties.

Monitor Interval (sec)	Specifies how often, in seconds, the monitor checks the Nagios server for status changes. Minimum value is 15 seconds.
Lag Tolerance (minutes)	Specifies, in minutes, how far into the past from the most recent triggered event, the activity should continue to monitor for new events that have yet to be reported.

Optional Properties

You can configure the following properties, as required.

Service Group Name	Specifies a service group to be monitored. The monitor will only trigger on service status changes for services which are part of this service group.

Filters

This activity provides the following filters, that you can combine as required, to selectively filter which service status records will trigger the monitor and be published to the Orchestrator data bus.

Active Checks Enabled	Filter by Active Checks Enabled value.
Check Command	Filter by Check Command value.
Current Check Attempt	Filter by Current Check Attempt.
Current State	Filter by Current State. Options include OK, WARNING, CRITICAL, and UNKNOWN.
Event Handler Enabled	Filter by Event Handler Enabled value.
Flap Detection Enabled	Filter by Flap Detection Enabled.
Has Been Checked	Filter by Has Been Checked value.
Host Address	Filter by Host Address value.
Host Display Name	Filter by Host Display Name.

Host ID	Filter by Host ID.
Host Name	Filter by Host Name.
Instance ID	Filter by Instance ID.
Is Flapping	Filter by Is Flapping value.
Is Pending	Filter by Is Pending value.
Notifications Enabled	Filter by Notifications Enabled value.
Passive Checks Enabled	Filter by Passive Checks Enabled value.
Problem Acknowledged	Filter by Problem Acknowledged value.
Service ID	Filter by Status ID.
Service Name	Filter by Service Name.
Service Status ID	Filter by Service Status ID.
State Type	Filter by State Type value.
Status Update Time	Filter by Status Update Time value.

Published Data

This activity publishes the following activity-specific items.

Acknowledgement Type	Acknowledgement Type. Possible values include NONE, NORMAL and STICKY.
Active Checks Enabled	Specifies if active checks are enabled or not.
Check Command	Check command.
Check Time Period ID	Check Time Period ID
Check Type	Type of check performed. Possible values include ACTIVE, PASSIVE, PARENT, FILE and OTHER.
Current Check Attempt	Current check attempt.
Current Notification Number	Current notification number
Current State	Current service state. Possible values include OK, WARNING, CRITICAL and UNKNOWN.
Event Handler	Event handler.
Event Handler Enabled	Specifies if event handler is enabled or not.
Execution Time (sec)	Check execution time in seconds.
Flap Detection Enabled	Specifies if flap detection is enabled or not.
Has Been Checked	Specifies if service has been checked or not.
Host Address	Host IP address.
Host Display Name	Host display.

Host ID	Host identifier.
Host Name	Host name.
Instance ID	Service status instance identifier.
Is Flapping	Specifies if flapping (state is changing too frequently) or not.
Is Pending	Specifies if status is pending or not.
Last Check	Date and time when last check was performed.
Last Hard State	Last hard state value. Possible values include OK, WARNING, CRITICAL and UNKNOWN.
Last Hard State Change	Last time when the hard state changed.
Last Notification	Time when last notification was sent.
Last State Change	Last time when the state changed.
Last Time Critical	Last time when the service status was Critical.
Last Time OK	Last time when the service status was OK.
Last Time Unknown	Last time when the service status was Unknown.
Last Time Warning	Last time when the service status was Warning.
Latency (sec)	Check latency in seconds.
Max Check Attempts	Maximum number of check attempts.
Modified Service Attributes	Bitmask value indicating which attributes have changed. See the remarks section below for details.
Next Check	Date and time when next check will be performed.
Next Notification	Date and time when next notification will be performed.
Normal Check Interval (min)	Number of minutes between checks.
Notifications Enabled	Specifies if notifications are enabled or not.
Obsess Over Service	Specifies if “obsessing” over service checks is enabled or not.
Passive Checks Enabled	Specifies if passive checks are enabled or not.
Percent State Change	Specifies the percent state change value.
Performance Data	Performance data.
Problem Acknowledged	Specifies if problem has been acknowledged or not.
Process Performance Data	Specifies if performance data should be processed or not.
Retry Check Interval (min)	Number of minutes between retires.
Scheduled Downtime Depth	Scheduled downtime depth.
Service ID	Service identifier.
Service Name	Service name.

Service Status Count	Number of records returned by the activity
Service Status ID	Service status identifier.
Should Be Scheduled	Should be scheduled.
State Type	Specifies state type. Possible values include HARD and SOFT.
Status Text	Status text description.
Status Text Long	Long status text description.
Status Update Time	Date and time when status was updated.

Remarks

The numeric value that is published for the **Modified Service Attributes** data item is a bitmask, in which each bit in the number has the following meaning.

Binary Value	Decimal Value	Meaning
0000 0000 0000 0000 0000	0	NONE
0000 0000 0000 0000 0001	1	NOTIFICATIONS ENABLED
0000 0000 0000 0000 0010	2	ACTIVE CHECKS ENABLED
0000 0000 0000 0000 0100	4	PASSIVE CHECKS ENABLED
0000 0000 0000 0000 1000	8	EVENT HANDLER ENABLED
0000 0000 0000 0001 0000	16	FLAP DETECTION ENABLED
0000 0000 0000 0010 0000	32	FAILURE PREDICTION ENABLED
0000 0000 0000 0100 0000	64	PERFORMANCE DATA ENABLED
0000 0000 0000 1000 0000	128	OBSESSIVE HANDLER ENABLED
0000 0000 0001 0000 0000	256	EVENT HANDLER ENABLED
0000 0000 0010 0000 0000	512	CHECK COMMAND
0000 0000 0100 0000 0000	1024	NORMAL CHECK INTERVAL
0000 0000 1000 0000 0000	2048	RETRY CHECK INTERVAL
0000 0001 0000 0000 0000	4096	MAX CHECK ATTEMPTS
0000 0010 0000 0000 0000	8192	FRESHNES CHECKS ENABLED
0000 0100 0000 0000 0000	16384	CHECK TIMEPERIOD
0000 1000 0000 0000 0000	32768	CUSTOM VARIABLE
0001 0000 0000 0000 0000	65536	NOTIFICATION TIMEPERIOD

Remove Acknowledgement Activity

The **Remove Acknowledgement** activity is used in a runbook to remove a host or service problem acknowledgement.

Required Properties

You must configure the following properties.

Host Name	Name of host with the problem acknowledgement (or host with a service which has a problem acknowledgement).
Object Type	Specifies the type of object whose problem acknowledgement is being removed. Options include HOST and SERVICE**.**
Service	Service with the problem acknowledgement.
Wait to Complete	Specifies whether the activity should wait for the acknowledgement to be removed, before completing. Use *Wait Timeout* to specify a timeout period. If configured to wait and *Wait Timeout* is not specified the activity waits until the acknowledgement has been removed.

Optional Properties

You can configure the following properties, as required.

Wait Timeout (sec)	Specifies how long the activity should wait for the acknowledgement to be removed, before completing. Use this property when **Wait to Complete** is set to **True**.

Published Data

This activity publishes the following activity-specific items.

Acknowledgement Removed	When *Wait To Complete* is set to *True*, this indicates whether the acknowledgement has been removed at the time when the activity completed.
Host Name	Host whose problem acknowledgement is being removed.
Object Type	Type of object whose problem acknowledgement is being removed.
Service	Service whose problem acknowledgement is being removed.

Schedule Downtime Activity

The Schedule Downtime activity is used in a runbook to schedule a host or service downtime period.

Tip: This is a "fire and forget" type activity with the downtime record being created some time after the activity completes. Use the Get Scheduled Downtime activity to verify that the downtime record has been created.

Required Properties

You must configure the following properties.

Author Name	Author scheduling the downtime.
Comment	Comment regarding scheduled downtime.
Downtime Scope	Specifies the scope of the downtime. See remarks for details.
Downtime Type	Specifies downtime type.
Duration Hours	Downtime hour duration component. Available when **Downtime Type** is FLEXIBLE
Duration Minutes	Downtime minute duration component. Available when **Downtime Type** is FLEXIBLE
End Time	Date and time when downtime should end.
Host Group Name	Name of host group for which downtime is to be scheduled. Available when **Downtime Scope** is HOSTGROUP_HOST or HOSTGROUP_SERVICE.
Host Name	Name of host for which downtime is to be scheduled. When scheduling downtime for a service, this specifies the host containing that service. Available when **Downtime Scope** is HOST or SERVICE.
Service Group Name	Name of service group for which downtime is to be scheduled. Available when **Downtime Scope** is SERVICEGROUP_HOST or SERVICEGROUP_SERVICE.
Service Name	Service with for which downtime is to be scheduled. This property is available when **Downtime Scope** is SERVICE.
Start Time	Date and time when downtime should start.

Optional Properties

You can configure the following properties, as required.

Triggered By	Specifies the Downtime ID of a scheduled downtime record that should trigger this downtime.

Published Data

This activity publishes the following activity-specific items.

Downtime Scope	Specifies the scope of the scheduled downtime. See remarks for details.
Host Group Name	Name of host group for which downtime has been scheduled.
Host Name	Name of host for which downtime has been scheduled.
Service Group Name	Name of service group for which downtime has been scheduled.
Service Name	Service for which downtime has been scheduled.

Remarks

When configuring the **Downtime Scope** property, the following values are supported. Similarly, when using the **Downtime Scope** published data item, the following values may be present.

- **HOST**. Single host
- **HOSTGROUP_HOST**. All hosts in host group
- **HOSTGROUP_SERVIC**E. All services in host group
- **SERVICE**. Single service
- **SERVICEGROUP_HOST**. All hosts containing services in service group.
- **SERVICEGROUP_SERVICE**. All services in service group