

Event Management Fundamentals

lab guide

Washington DC edition

© COPYRIGHT 2024 SERVICENOW, INC. ALL RIGHTS RESERVED.

ServiceNow provides this document and the information therein “as is” and ServiceNow assumes no responsibility for any inaccuracies. ServiceNow hereby disclaims all warranties, whether written or oral, express or implied by law or otherwise, including without limitation, any warranties of merchantability, accuracy, title, non-infringement or fitness for any particular purpose.

In no event will ServiceNow be liable for lost profits (whether direct or indirect), for incidental, consequential, punitive, special or exemplary damages (including damage to business, reputation or goodwill), or indirect damages of any type, however, caused even if ServiceNow has been advised of such damages in advance or if such damages were foreseeable.

TRADEMARKS

ServiceNow and the ServiceNow logo are registered trademarks of ServiceNow, Inc. in the United States and certain other jurisdictions. ServiceNow also uses numerous other trademarks to identify its goods and services worldwide. All other marks used herein are the trademarks of their respective owners and no ownership in such marks is claimed by ServiceNow.

Contents

Overview Event Generator and Event Test	Lab	1.1	⌚15m	4
Overview Explore Guided Setup Validate the MID Server	Lab	1.2	⌚10m	10
Architecture Create Application Services	Lab	2.1	⌚30m.....	17
Architecture Create a Dynamic CI Group	Lab	2.2	⌚15m.....	29
Architecture Execute a Discovery and Bind with IP and MAC	Lab	2.3	⌚20m	37
Event Management Event Processing	Lab	3.1	⌚25m.....	46
Event Management CI Binding with Event Rules	Lab	3.2	⌚20m.....	57
Event Management Event Rule Thresholds	Lab	3.3	⌚40m.....	74
Event Management Event Binding with Event Rules and CI Field Matching	Lab	3.4	⌚35m	83
Event Management Event Field Mapping Rules	Lab	3.5	⌚20m	94
Alerts and Tasks Navigate Service Operations Workspace	Lab	4.1	⌚20m	99
Alerts and Tasks Alert Management Rules	Lab	4.2	⌚20m	111
Alerts and Tasks Configure the Service Map	Lab	4.3	⌚20m	132
Alerts and Tasks Application Service SLAs	Lab	4.4	⌚15m.....	144
Event Sources Create SolarWinds Connector	Lab	5.1	⌚20m	150
Event Sources Processing Events from an Email Source	Lab	5.2	⌚25m.....	162
Event Sources Capture and Process SNMP Traps	Lab	5.3	⌚30m	172
Event Sources Use Agent Client Collector Monitoring	Lab	5.4	⌚45m	186

Overview

Event Generator and Event Test

Lab

1.1

15m

Lab Objectives

You will achieve the following objectives:

- Use the Event Generator (simulation application) to test the configuration.

Scenario

In this course, you will use the event generator to simulate the arrival of a new event. The event generator simulates various event sources providing event data directly to the event table in your ServiceNow instance.

IMPORTANT NOTE: Login information for your personal ServiceNow instance and Windows MID Server are found on the Now Learning course page. The MID SERVER PASSWORD shown is also your ServiceNow instance **admin** account password.

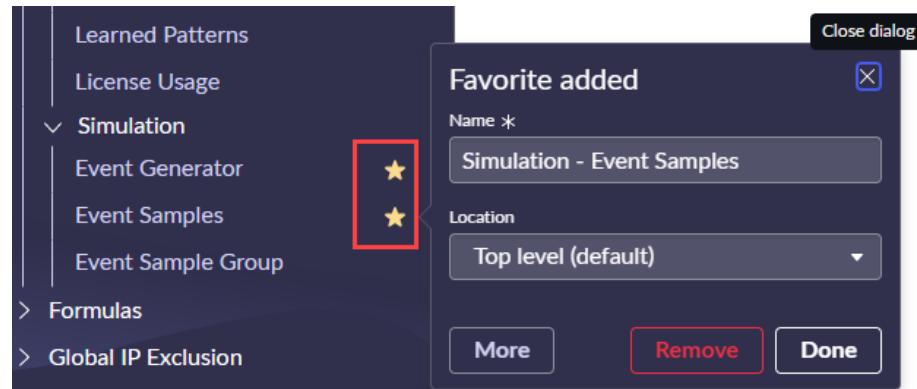
Access the course page in Now Learning to request and access your lab environment.

The screenshot shows the 'Event Management Fundamentals On Demand (Tokyo)' course page. On the left, there's a sidebar with a tree view of course content. A red box highlights the 'Lab Guide Download (T)' link under the 'Lab Guide (T)' section. A red arrow points from this link to the 'MID SERVER PASSWORD' field on the right side of the page. The 'MID SERVER PASSWORD' field contains the placeholder 'Lwi...z2k (Username: Administrator)'. The right side of the page also displays the 'MID SERVER RDP URL' (nowlearning-nlinserv...20-mid-001.lab.service-now.com), 'INSTANCE STATUS' (Running), and a note about instance expiration.

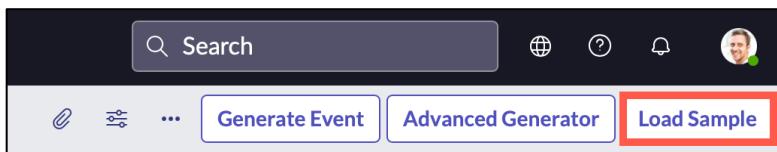
A. Confirm Event and Associated Alert are Generated in Your ServiceNow Instance

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.

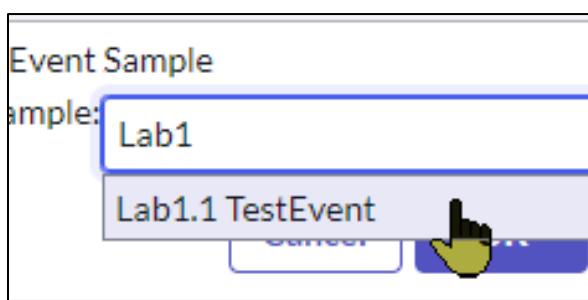
Tip: Click the star to the right of the Event Generator AND Event Samples to add them to your Favorites list for quick future access.



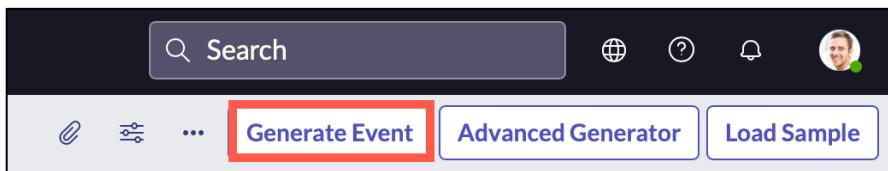
2. In the upper right, click **Load Sample**.



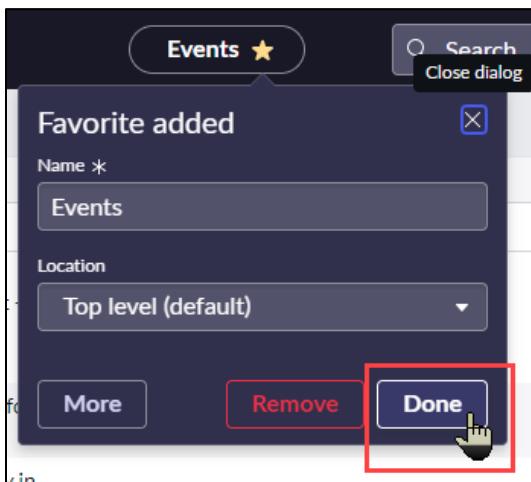
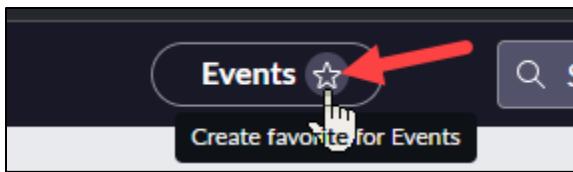
3. In the Choose Event Sample dialog box, enter **Lab1** and wait for the filtered list.
4. From the list, select **Lab1.1 TestEvent** and click **OK**.



5. Review the sample event then click **Generate Event**.



6. You are redirected to All Events. **Refresh** the list to see the event just fired.
7. Use the Contextual app pill in the menu bar to **favorite** the Events list.



- From the menu on the **Time of event** column, click **Sort (z to a)**.

Time of event	Source	Description
2022-01-11 22:42:08		
2022-01-11 22:48:47		

Note: This sorts the events list by the latest recorded event; your new event should be near the top. You may also see a series of events with a Source of EMSelfMonitoring. These are generated by Event Management self-health monitoring.

- Observe the created event.

Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key	State
2022-01-11 22:42:08	PSScript	This is a Test for Lab 1.1			SNDemo		1-1HT2017	Processed

- Click on the link in the **Time of event** column to open the event and scroll down to the Alert field.

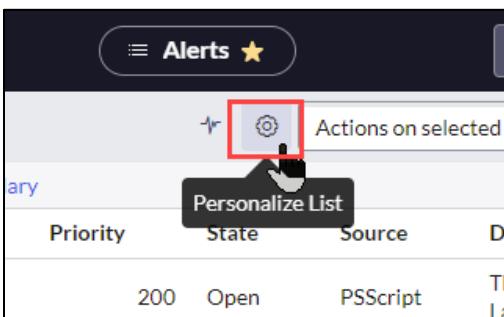
Alert	Alert0010004
Description	This is a Test for Lab 1.1
Additional information	Welcome to Event Management Fundamentals!
Processing Notes	<p>Binding alert CI process flow:</p> <p>Event CI type is empty</p> <p>No CI found for binding (Failed to resolve the event node to CI id)</p> <p>Binding Failure Reason: Validate existing event rules of "PSScript" source for binding metric events</p>

Note: An alert generates, and the event-processing engine creates Processing Notes. The engine could not find an associated CI for the event; thus, the alert is “unbound”. Your alert number may differ from that shown here.

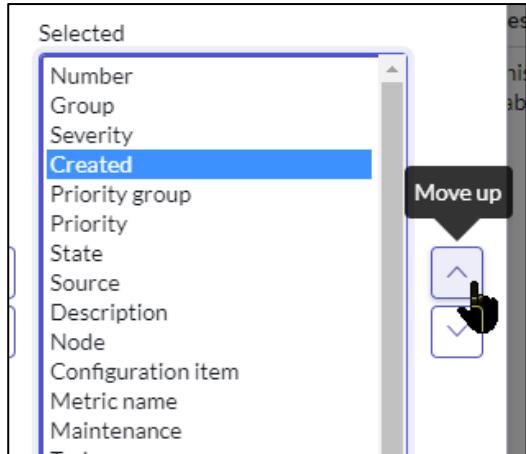
11. Navigate to Event Management > All Alerts.

Note: Use the Contextual app pill in the menu bar to **favorite** the Alerts list.

12. Click the **Personalize List** icon and add **Created** to the Selected column.



13. Using the **Move up** arrow to the right of the **Selected** pane, position **Created** after **Severity**.



14. Click **OK**.

15. Sort the list by the **Created** column by clicking on the column header.

	Number	Group	Severity	Created	Priority group	Priority	State
<input type="checkbox"/>	Alert0010004		Minor	2022-01-11 22:42:18	High	200	Open

Note: An alert generates from the event with Source **PSScript**.

16. Open the alert with the source of PSScript.

Number	Alert0010004	Severity	Minor
Source	PSScript	State	Open
Type	SNDemo	Acknowledged	<input type="checkbox"/>
Resource		Maintenance	<input type="checkbox"/>
Configuration item		Updated	2022-01-24 23:32:59
Task		Parent	
Metric name		Knowledge article	
Description	This is a Test for Lab 1.1	Overall Event Count	1
Message key	1-1HT2017		

Note: Fields populated by the event include: Source, Type, Description, Message key, and Severity. An alert is the actionable piece of Event Management.

17. Scroll down to the Related Search Results section and select the **More Information** tab.

The screenshot shows the ServiceNow Event Management interface. At the top, there is a navigation bar with tabs: Impacted Services, Flapping, History, Activities, More Information (which is highlighted with a teal background), Repeated Alerts, Similar Alerts, CI Incidents, and CI Changes. Below the navigation bar, there are three sub-tabs: Related Incidents, Related Change Requests, and Related Problems. The main content area displays a 'Priority Breakdown' section. It states: 'The Alert Priority score 200020.001 was calculated according to the following factors, ordered by their respective priority (2021-09-20 21:09:57 GMT)'. It then lists six categories with their scores and weights: 1. Business services - (0), 2. Severity - (2.0, 100000.0), 3. Ci type - (0), 4. Role - (2.0, 10.0), 5. Secondary - (0), and 6. State - (1.0, 0.001). At the bottom of the page, there is a large green button labeled 'Next Step'.

Priority Breakdown

The Alert Priority score 200020.001 was calculated according to the following factors, ordered by their respective priority (2021-09-20 21:09:57 GMT)

Category (Score, Weight)

1. Business services - (0)
2. Severity - (2.0, 100000.0)
3. Ci type - (0)
4. Role - (2.0, 10.0)
5. Secondary - (0)
6. State - (1.0, 0.001)

Additional information

```
{  
    "additional_content" : "Welcome to Event Management Fundamentals!"  
}
```

Congratulations on completing the lab!

Overview

Explore Guided Setup Validate the MID Server

Lab

1.2

10m

Lab Objectives

You will achieve the following objectives:

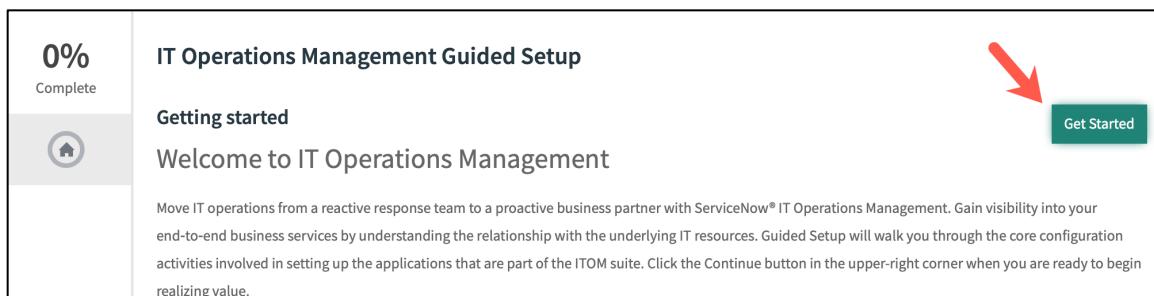
- Explore the ITOM Guided Setup application and use it to validate the MID Server

Scenario

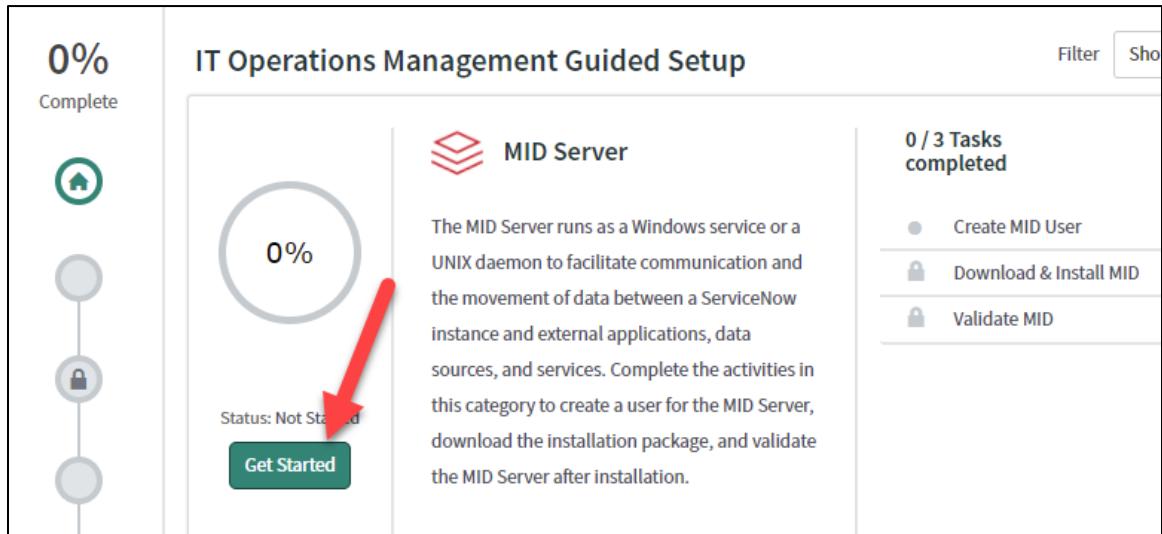
ITOM Guided Setup helps in your Event Management deployment. Explore its features and use the MID Server setup to validate the preinstalled MID Server. More information about the MID Server will be covered in the next lesson.

A. Explore ITOM Guided Setup

1. Navigate to **Guided Setup - Legacy > ITOM Guided Setup**
2. Review the landing page, then click **Get Started**.



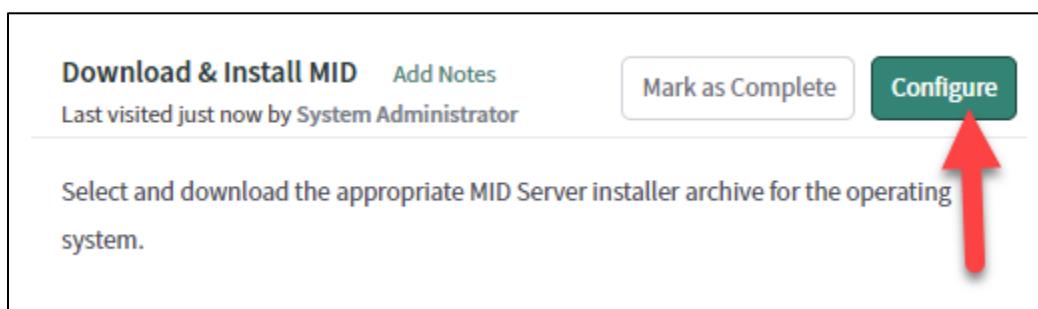
3. Since many ITOM products depend on the MID Server, it is at the top of the stack. Review the applications available for Guided Setup.
4. The MID User has already been created and the MID Server has already been installed, but the instance is not aware of this since it was done through automation of your class environment. In the MID Server section, click **Get Started**.



5. Next to Create MID User, click **Mark as Complete**.

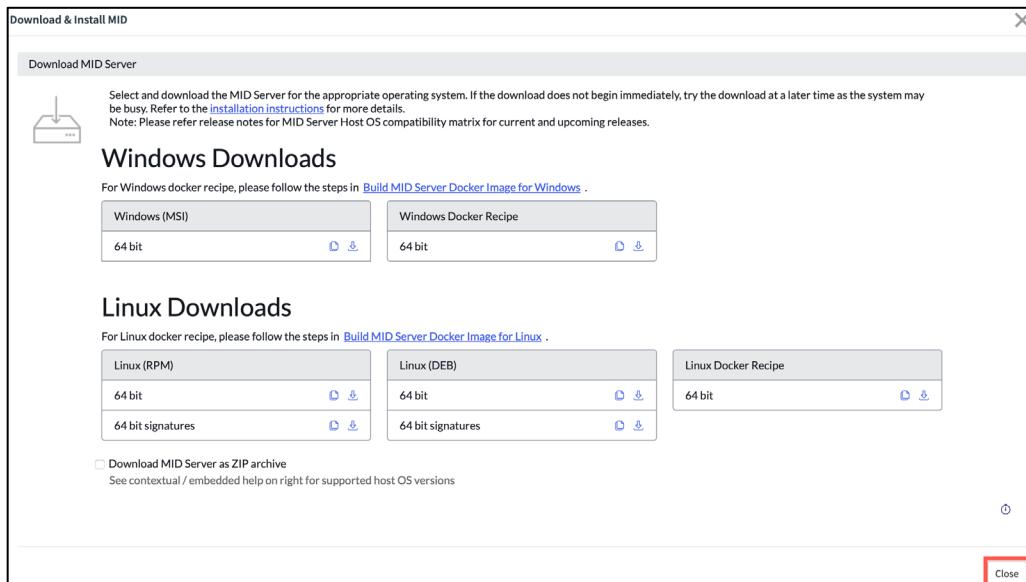


6. Next to Download and Install MID, click **Configure**.

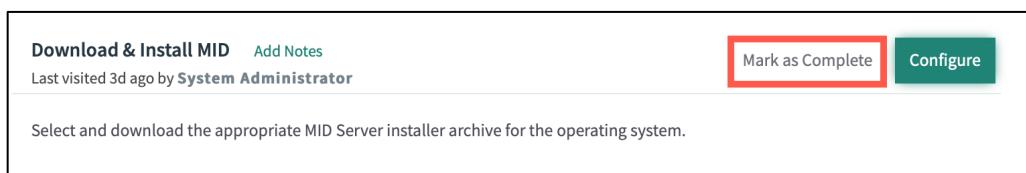


7. Review the available download packages. You can connect to this page from the server you plan to install the MID software on or download and transfer it. Click

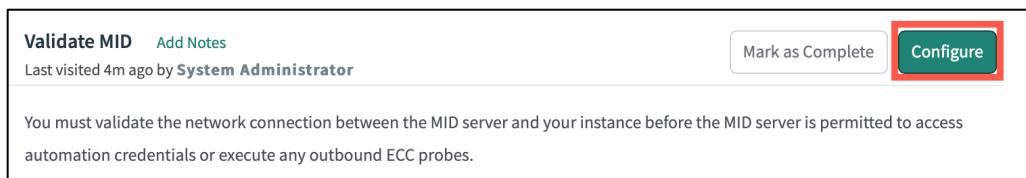
Close or browser back button.



8. Click **Mark as Complete.**



9. You should now show 2/3 tasks completed. Next to Validate MID, click **Configure.**

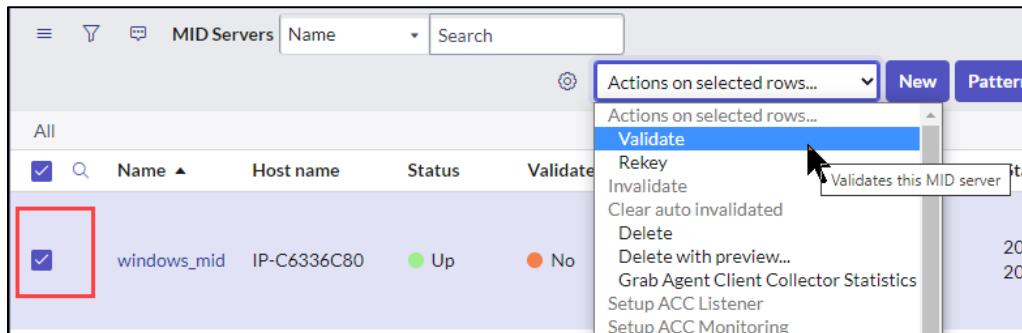


Note: The MID server list opens showing the single MID installed named **windows_mid**. Note that this MID is not yet validated.

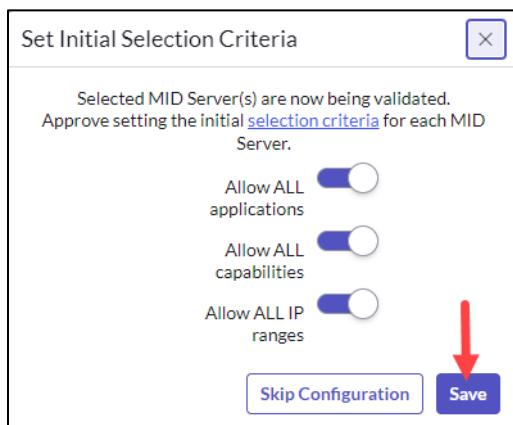
The screenshot shows the 'MID Servers' list. At the top, there are filter icons and a search bar. The table has columns: Name, Host name, Status, Validated, and Version. One row is shown for 'windows_mid' with the following details: Host name 'IP-C6336C80', Status 'Up', Validated 'No' (highlighted with a red box), and Version '1.0'.

Name	Host name	Status	Validated	Version
windows_mid	IP-C6336C80	Up	No	1.0

10. Check the box next to the MID (hover over to appear), and from the Actions menu, select **Validate**.



11. Leave the ALL defaults and click **Save**.



12. After about 1 minute, refresh the list. Confirm **Validated = Yes**.

Name	Host name	Status	Validated
windows_mid	IP-C6336C80	Up	Yes

13. Open the MID record by clicking the name.

Name	Host name	Status	Validated
windows_mid	IP-C6336C80	Up	Yes

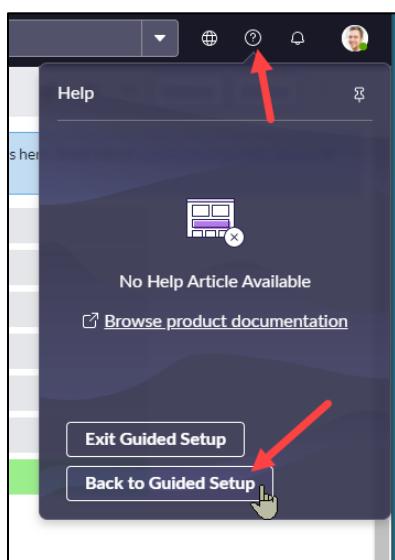
14. Locate the **IP address** field and save the private (internal) IP address of the MID for subsequent labs.

MID Server
windows_mid

MID Server facilitates communication between the ServiceNow platform and external applications, data sources, and services. Add M meters and capabilities here. Read about [configuring the MID Server](#) or find assistance with [MID Server troubleshooting](#).

Name	windows_mid	Host name	IP-C6336C80
Status	Up	IP address	198.51.100.110
Validated	Yes	Router	198.51.0.1

15. Click **Show Help** icon then **Back to Guided Setup**.



16. In guided setup, validate MID section, click **Mark as Complete**.

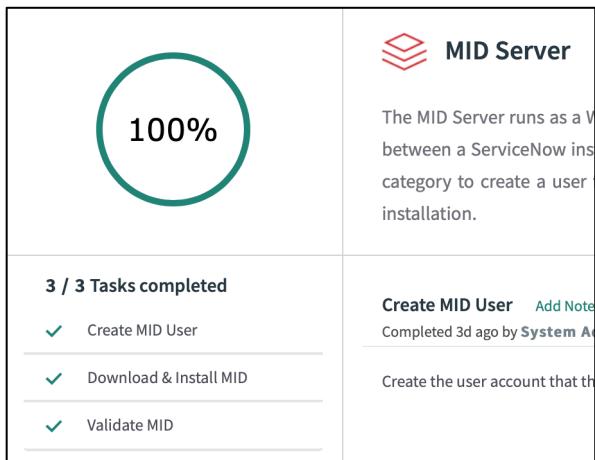
Validate MID [Add Notes](#)

Last visited 26m ago by **System Administrator**

You must validate the network connection between the MID server and your instance before the MID server is permitted to access automation credentials or execute any outbound ECC probes.

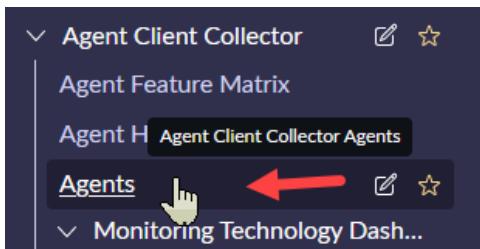
[Mark as Complete](#) [Configure](#)

17. MID Server should now show 100%.



B. Validate ACC Agent Installation

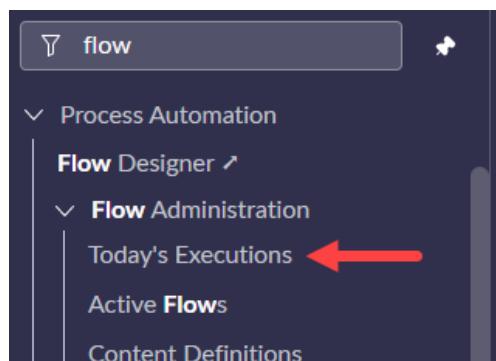
1. Navigate to **Agent Client Collector > Agents**.



2. The ACC agent installation takes approximately 5 minutes to complete after validating the MID. You should see 1 agent **Up** with Host data **Collected** in the list.

Name	Status	Host data collection	Host	Class	Mid	IP Address
Agent_IP-C6334B4E	Up	Collected	ip-c6334b4e	Windows Server	windows_mid	198.51

3. You can see the flow execution that installs the ACC agent with **Process Automation > Flow Designer > Flow Administration > Today's Executions**.



Flow engine contexts					
	Created	Name ▲	State	Runtime	Created by
<input type="checkbox"/>	2023-01-23 18:52:18	InstallIACConMID	Complete	6,852	lab.midserver
	2023-01-23 18:19:12	Show Alert Executions	Complete	886	system
	2023-01-23 18:19:09	Show Alert Executions	Complete	791	system



Congratulations on completing the lab

Architecture

Create Application Services

Lab
2.1
30m

Lab Objectives

You will achieve the following objectives:

- Set existing application service's criticality and status
- Generate an infrastructure event against a node within an application service
- Navigate the Event Management Service Operations Workspace
- Navigate application service maps

Scenario

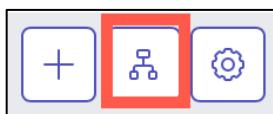
In this lab, two manually created application services have been defined on your lab instance based on CIs in your CMDB. *Business criticality* and *operational status* have not been set. Set those fields to define how the applications appear in Service Operations Workspace. Fire a sample event against a node within one of the application services to view how the overall Event Management process operates.

Note: *These example services are used for demonstration purposes throughout the remainder of the class.*

A. Update application services for display in Service Operations Workspace

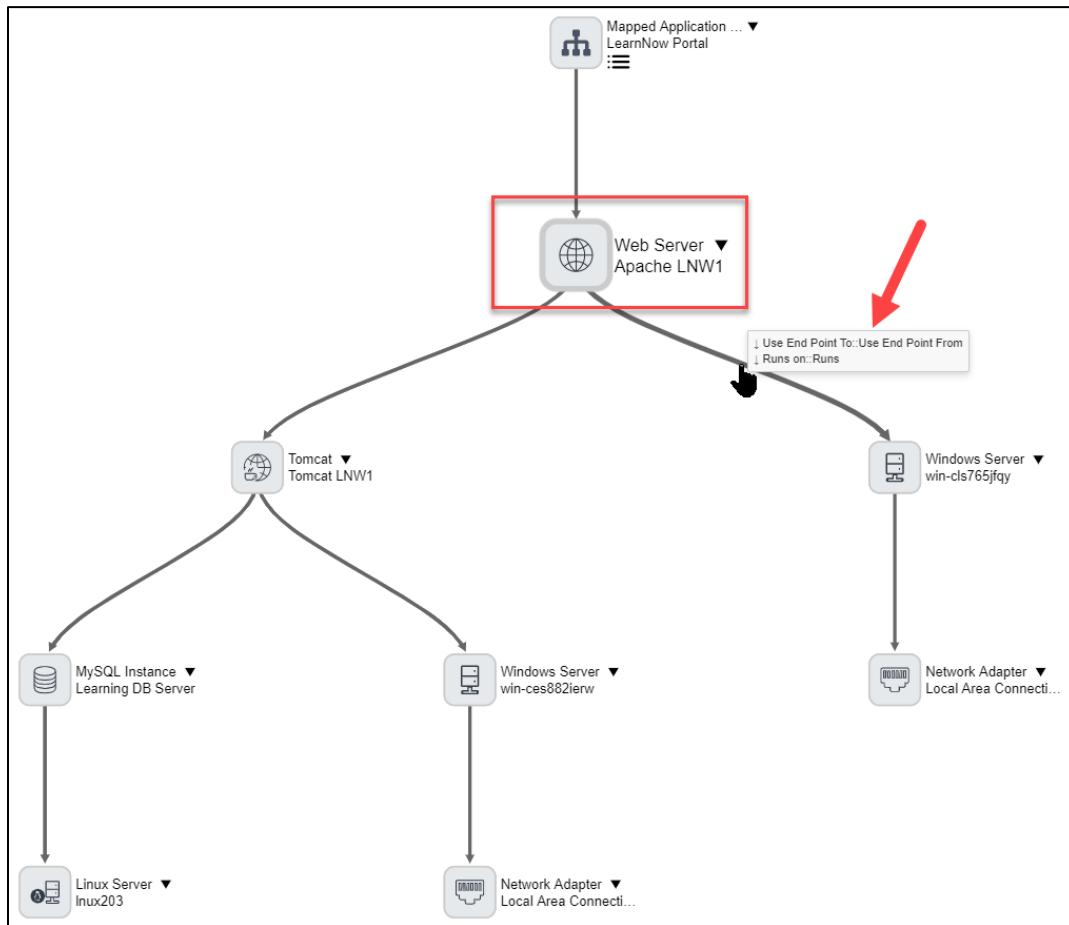
In this section, configure 2 application services for display in Service Operations Workspace.

1. In your ServiceNow instance, navigate to **Configuration > Application Servers > Web Servers**.
2. Open the Web Server **Apache LNW1**.
3. In the Related Items gray bar, click the **Show dependency views** icon.



Note: *This opens the dependency map in a new tab.*

4. Observe the dependency map.



Note: The Apache LNW1 web server runs on a Windows server with the name **win-cls765jfqqy**.

5. Close the map tab and navigate to **Event Management > Services > Application Services**.
6. The default view only shows *operational* services. **Remove the filter condition** to display all services.

The screenshot shows the 'Mapped Application Services View' interface. At the top, there are filter icons for 'All', 'Operational status = Operational', and 'Name'. A button labeled 'Remove next condition' is highlighted with a black box and a cursor icon. Below the filters is a table header with columns 'Name' and 'View Service'.

7. Click **LearnNow Portal** from the list.

All	Name	View Service
ServiceNow Event Management	View Service	
LearnNow Portal	View Service	
SurveyProject	View Service	

8. Update the **Additional Info** section to 2- somewhat critical and Operational.

Additional Info

Business criticality	Traffic based discovery
2 - somewhat critical	<input checked="" type="checkbox"/>
Operational status	Comments
Operational	

Note: There is no mechanism or API that automatically updates application services that were created manually. You can only update application services which contain manually created entry points by using the related link "Update with changes from CMDB."

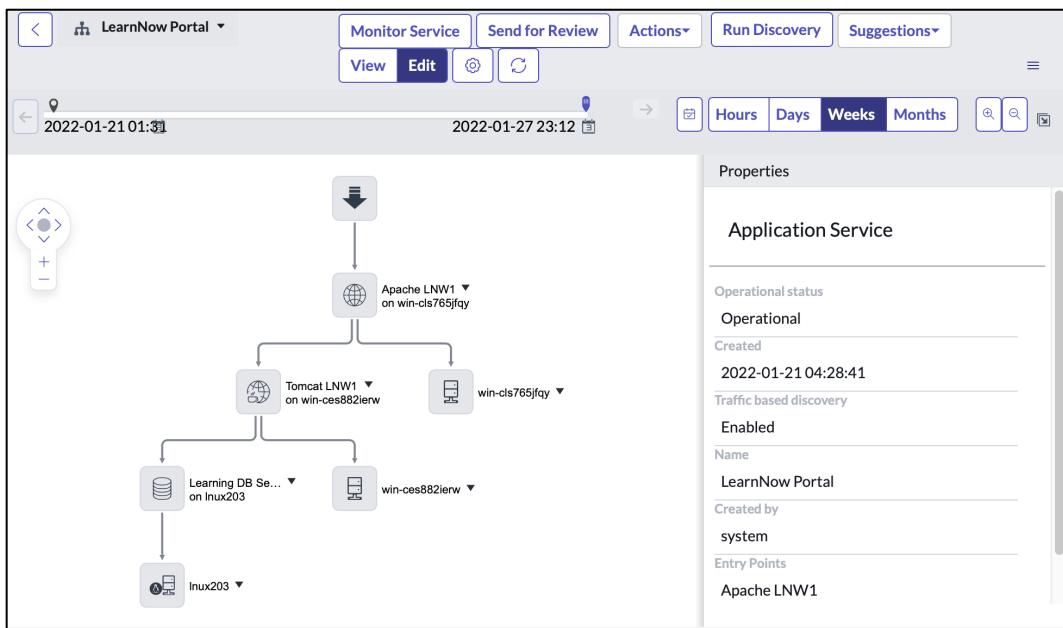
9. Click **Update**. A success message will be presented.

Application service updated successfully.

LearnNow Portal

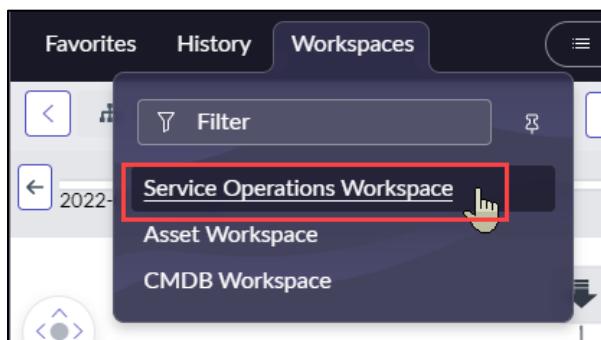
10. At the upper right of the form, select **View Map**.

Delete Service Actions Update View Map

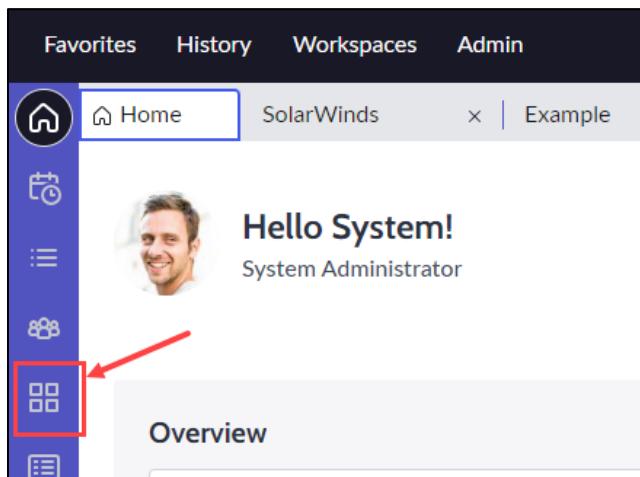


█ Note: This displays the service/topology map of your application service.

11. In the **Workspaces** menu, click **Service Operations Workspace**.



12. In Service Operations Workspace (SOW), click the **Service Dashboard** tab.

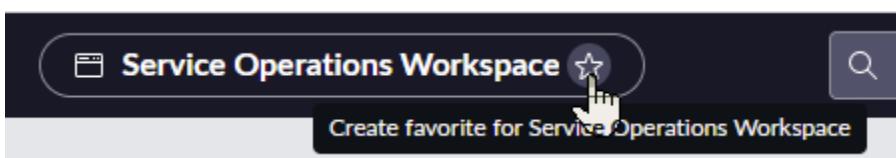


13. The service appears in SOW because its operation status is set to operational.

A screenshot of the Service Dashboard in the Service Operations Workspace. The dashboard title is "Default | 2 services". It shows a severity breakdown with 0 Critical (0%), 0 Major (0%), 0 Minor (0%), and 1 OK (50.0%). Below this, there are filters for grouping by Business criticality (set to Ascending) and segmenting by Severity. The main list shows two services: "2 - somewhat critical (1)" which includes "LearnNow Portal" (marked with a green checkmark) and "4 - not critical (1)" which includes "ServiceNow Event Management". There's also a "Search services" input field.

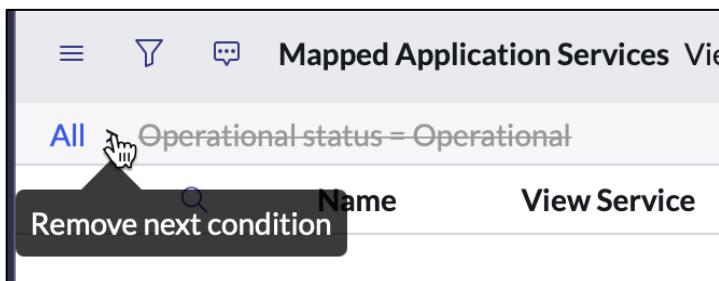
Note: The ServiceNow Event Management service appears as part of self-health monitoring.

14. Add the Service Operations Workspace service dashboard to your favorites for quick future access.



15. Navigate to **Event Management > Services > Application Services**.

16. Remove the filter condition to display all services.



17. Click **SurveyProject** from the list.

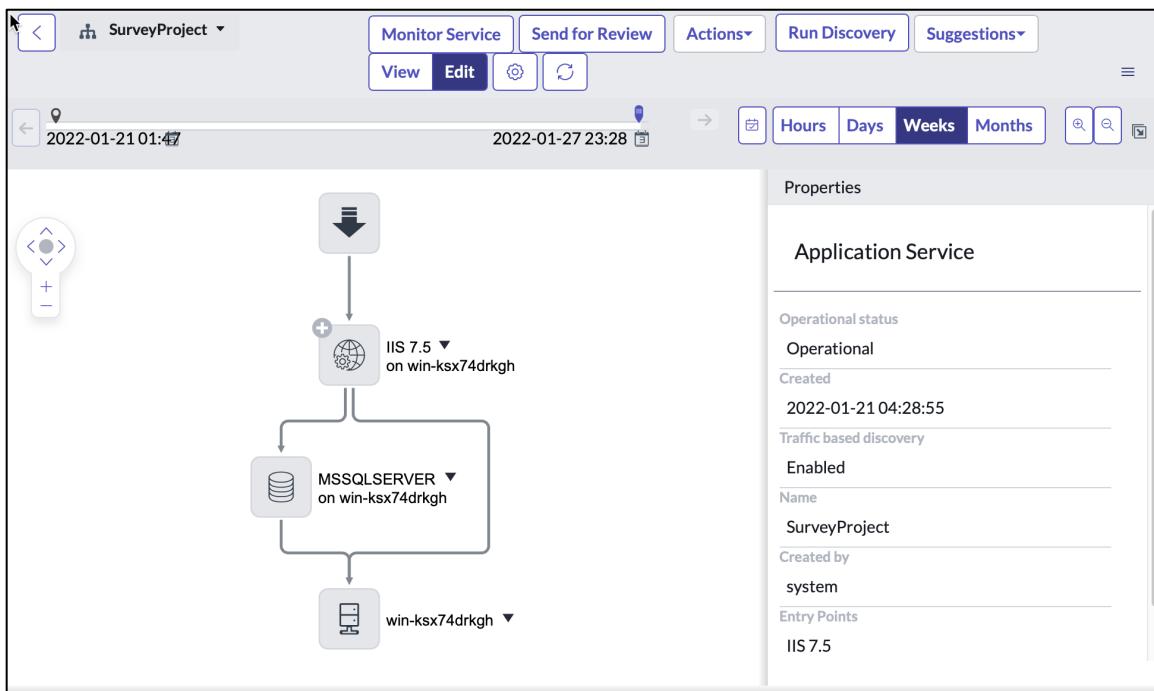
All	Name	View Service
	ServiceNow Event Management	View Service
	LearnNow Portal	View Service
	SurveyProject	View Service

18. Update the Additional Info to **3 – less critical** and **Operational**. Click **Update**.

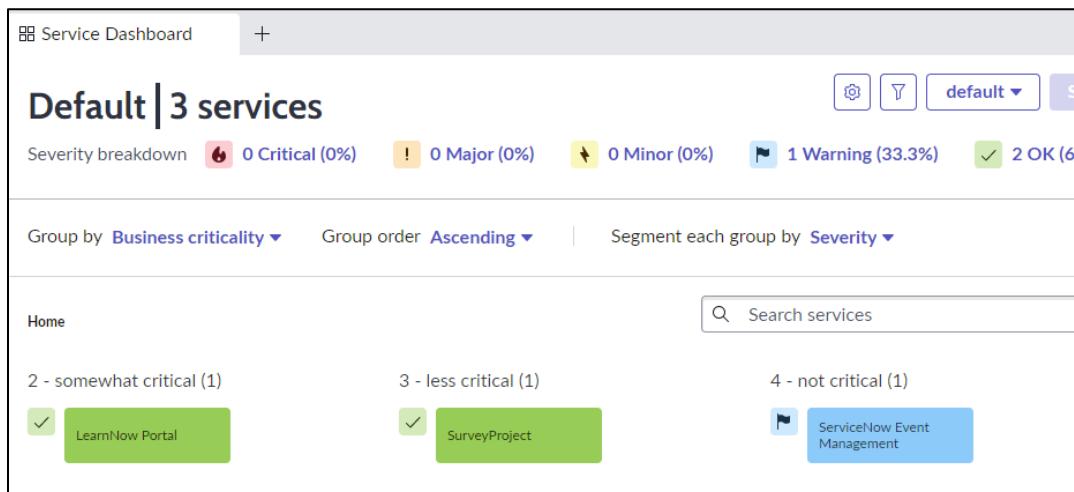
A screenshot of a "Additional Info" update form. At the top, there is a toolbar with icons for "Delete Service", "Actions", "Update" (which is highlighted with a red box), and "View Map". Below the toolbar, the section title "Additional Info" is displayed. There are two main sections: "Business criticality" and "Operational status". The "Business criticality" section contains a dropdown menu with the option "3 - less critical" selected. The "Operational status" section also contains a dropdown menu with the option "Operational" selected. To the right of these sections, there is a checkbox labeled "Traffic based discovery" which is checked.

19. At the upper right of the form, click **View Map**.





20. Return to the **Service Operations Workspace** service dashboard to view the three operational services.



B. Generate an infrastructure event against the Apache host server and the LearnNow Portal

In this section, generate an infrastructure event against the Apache host server and the LearnNow Portal.

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator** (use your favorites).
2. In the upper right, click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab2** and wait for the filtered list.
4. From the list, select **Lab2.1 EventWinLNW** and click **OK**.
5. Click **Generate Event**.
6. You are redirected to All Events. **Refresh** the list until the State is **Processed**.
7. Open the latest event and observe the **Node** and **Processing Notes**.

Processing Notes	Binding alert CI process flow: Node will be resolved to CI id: 7e7453c1f8c223007f44536cf8b7b17f : found by node name Event CI type is empty No related CI found for binding, alert CI will be bound to node (id): 7e7453c1f8c223007f44536cf8b7b17f Bind to 7e7453c1f8c223007f44536cf8b7b17f
------------------	---

Note: *The latest event is at the top of the list due to sorting on Time of event.*

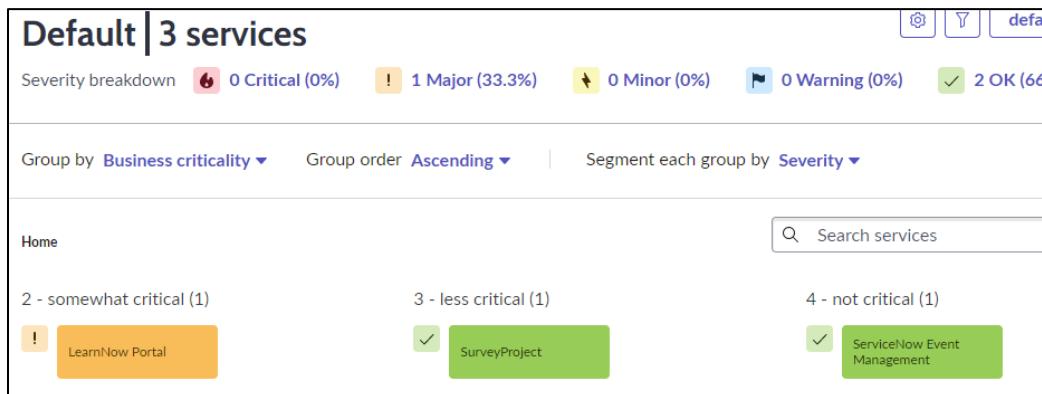
8. Navigate to **Event Management > All Alerts**.

Number	Group	Severity	Created	Priority group	Priority	State	Source	Description	Node	Configuration item
Alert0010005		Major	2022-02-09 04:30:39	High	3306	Open	PSScript	Issue on win-cls765jqy	win-cls765jqy	win-cls765jqy
Alert0010004		Minor	2022-02-09 03:37:33	High	200	Open	PSScript	This is a Test for Lab 1.1	(empty)	
Alert0010002		Minor	2022-02-08 21:33:29	High	200	Closed	EMSelfMonitoring	There is an error in the MID server: Use...		MID Servers

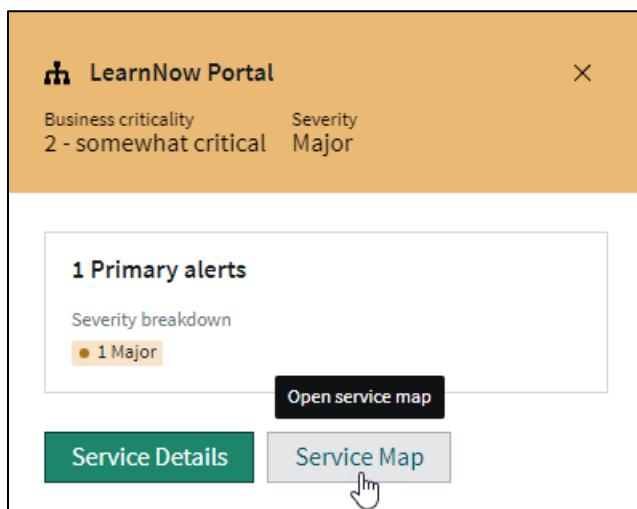
Note: *An alert generates and binds to a Configuration Item (CI) based upon the Node name **win-cls765jqy**. The alert number and Priority group may differ from that shown here.*

C. Observe the Service Operations Workspace and Event Management Application Service Map

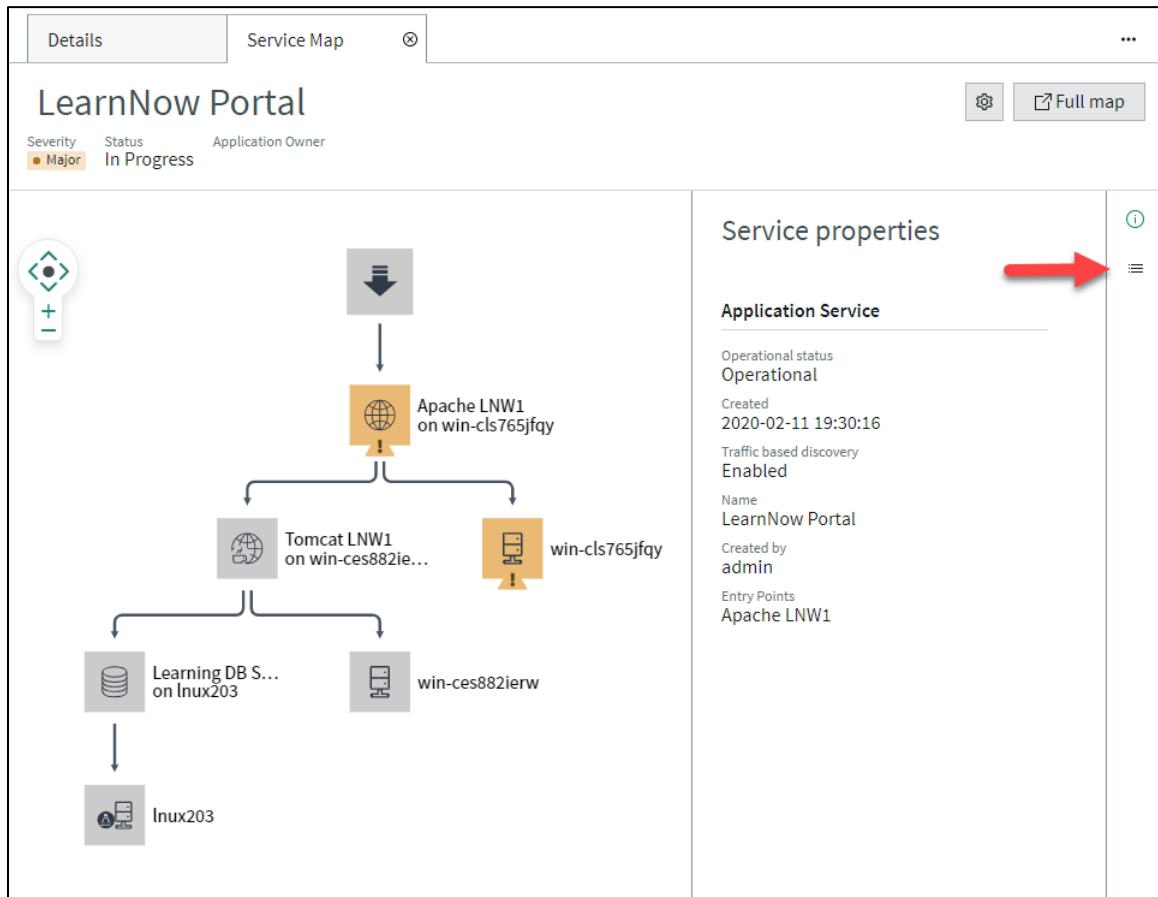
1. Navigate to **Service Operations Workspace** service dashboard.



2. Click the **LearnNow Portal** tile to open its service tab, then click **Service Map**.



Note: The Event Management service map opens in a new tab within Service Operations Workspace.



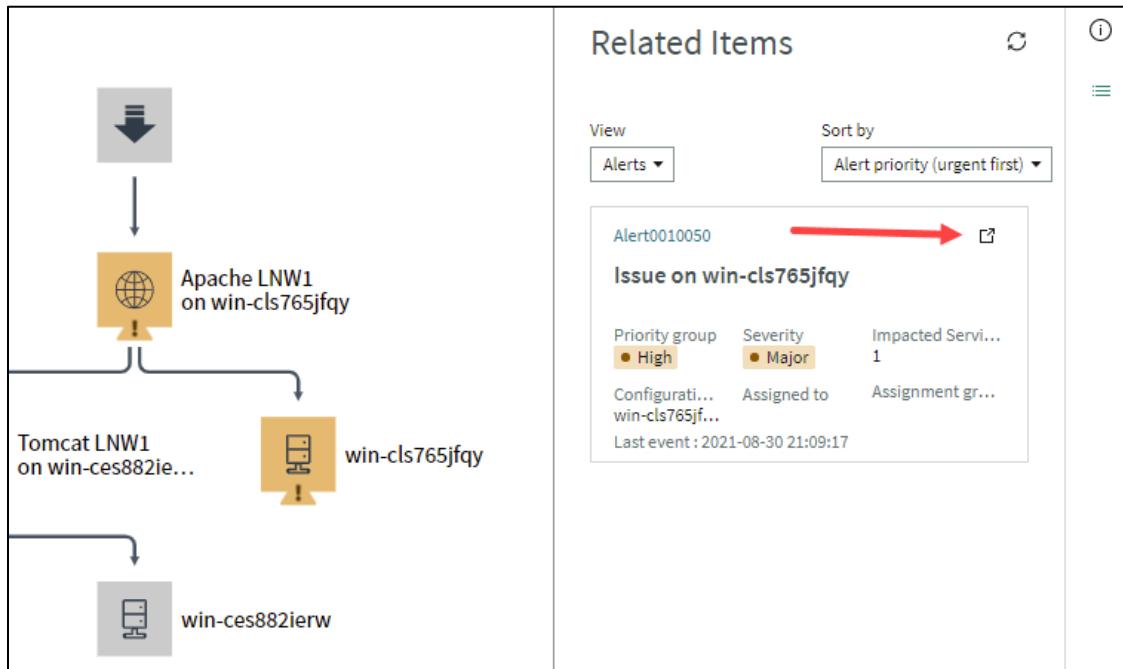
Note: Both the Windows Server and Apache Web Server are showing in a Major state as the Apache Web Server is running on win-cls765jfqy and is directly impacted by it. Only the Event Management service maps include alert effecting CI indicators.

3. Click **Related Items** to toggle from service properties.

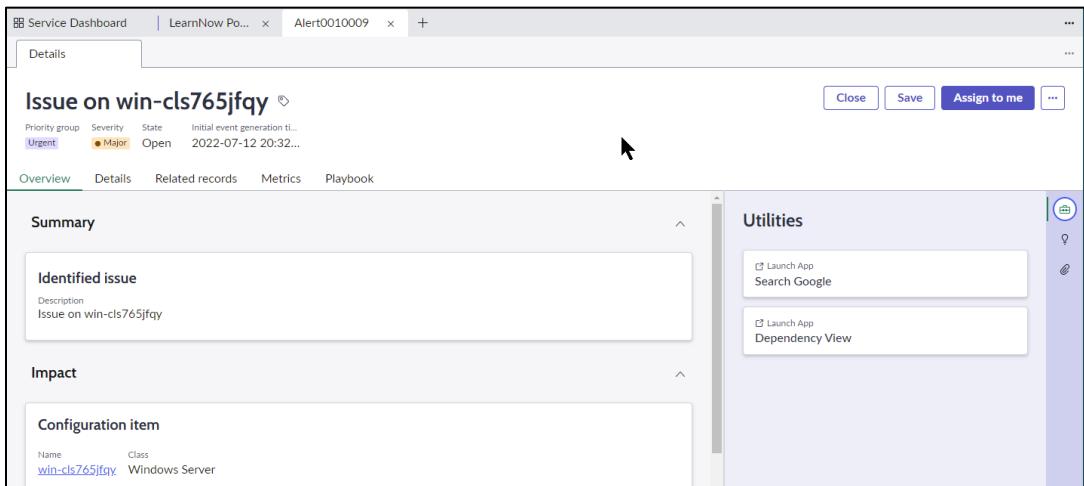
The image shows two views of the 'Related Items' feature. On the left, the 'Service properties' panel is shown with a red box highlighting the 'Related Items' button. On the right, the 'Related Items' panel is displayed, showing a specific alert entry:

Alert0010050		
Issue on win-cls765jfqy		
Priority group	Severity	Impacted Servi...
High	Major	1
Configurati...	Assigned to	Assignment gr...
Last event : 2021-08-30 21:09:17		

4. Investigate the **View** and **Sort by** menus, and use the **Open Record form**  icon to open the alert in a new workspace tab.



5. Review the information and tabs available in alert intelligence. Metric collection is not yet enabled.



The screenshot shows the 'Details' tab of the 'Issue on win-cls765jfqy' record. The top bar includes tabs for 'Service Dashboard', 'LearnNow Po...', 'Alert0010009', and '+'. Below the tabs, the 'Details' section displays the issue summary: 'Issue on win-cls765jfqy' (Priority group: Urgent, Severity: Major, State: Open, Initial event generation time: 2022-07-12 20:32...). The 'Overview' tab is selected, showing sections for 'Summary' (Identified issue: 'Issue on win-cls765jfqy') and 'Impact' (Configuration item: Name: win-cls765jfqy, Class: Windows Server). To the right, there is a 'Utilities' sidebar with links: 'Launch App' (Search Google) and 'Dependency View'.

6. Return to the service dashboard tab.

The screenshot shows the Service Dashboard with the following details:

- Services:** 3 services
- Severity breakdown:** 0 Critical (0%), 1 Major (33.3%), 0 Minor (0%), 0 Warning (0%), 2 OK (66.7%)
- Group by:** Business criticality
- Group order:** Ascending
- Segment each group by:** Severity

The services listed are:

- 2 - somewhat critical (1):** LearnNow Portal (orange card)
- 3 - less critical (1):** SurveyProject (green card)
- 4 - not critical (1):** ServiceNow Event Management (green card)

Note: The application services are displayed. They may appear differently based on your browser size.

Challenge Task: Change Prioritization of Items on Service Operations Workspace

Use the **Group by** and **Group order** dropdowns to change the default setting of the Event Management Service Operations Workspace. How do you explain the behavior you are seeing?

The screenshot shows the Service Dashboard with the 'Group by' dropdown open, revealing the following options:

- No grouping
- Severity
- Business criticality (selected)
- Location
- Service group...

The 'Group order' and 'Segment each group by' dropdowns are also visible with their respective red circles.



Congratulations on completing the lab!

Architecture

Create a Dynamic CI Group

Lab
2.2
15m

Lab Objectives

You will achieve the following objectives:

- Create a CMDB group of database CIs
- Create a dynamic CI group technical service
- Generate a test event against the dynamic CI group

Scenario

The dynamic CI group method for populating a service is based on a CMDB group. The members of the specified CMDB group comprise the service. The dynamic CI group continuously synchronizes with the CMDB group to reflect any changes in group membership.

In this lab, you create a CMDB group of databases, then use that CMDB group to create a dynamic CI group. You then generate an example event against one of the database CIs to view how the overall Event Management process operates on dynamic CI groups.

Note: This example service is also used for demonstration purposes throughout the remainder of class and represents another common type of service you may see in your company-specific Event Management configuration.

A. Create a CMDB Group

1. Navigate to Configuration > CMDB Groups.
2. Review the baseline CMDB groups, which are used in CI Overview in the CMDB Workspace.
3. Click **New**.



4. Set **Group Name** to **MyDatabases** and Save.

CMDB Group
New record

* Group Name: MyDatabases

Group type: Default

Submit

Save

- Configure >
- Export >
- Create Favorite
- Copy URL
- Copy sys_id
- Reload form

5. On the **CMDB Group Contains Encoded Queries** tab, click **New**.

Show All CI Delete

B Group Contains Saved Queries CMDB Group Contains Encoded Queries CMDB Group Contains Configuration Items

Class Search

up = MyDatabases

Class	Condition	Domain

New

6. In the **Class** field, select **Database [cmdb_ci_database]**.

CMDB Group Contains Encoded Query
New record

Simple Condition Add Filter Condition Add "OR" Clause

-- choose field -- -- oper -- -- value --

Condition Add Filter Condition Add "OR" Clause

-- choose field -- -- oper -- -- value --

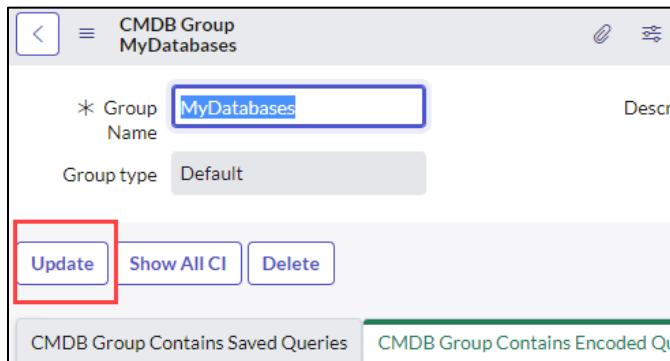
Domain global * Group MyDatabases

* Class Database [cmdb_ci_database]

Note: The *Class* field may appear in a different location on the form. Additional filter conditions are available when required.

7. Click **Submit**.
8. Click **Show All CI**. Thirteen (13) records should be returned.

9. Click **back icon**  then click **Update**.



CMDB Group
MyDatabases

* Group Name: MyDatabases

Group type: Default

Update Show All CI Delete

CMDB Group Contains Saved Queries CMDB Group Contains Encoded Qu

B. Create a Dynamic CI group and Display it in Service Operations Workspace

1. Navigate to **Event Management > Services > Dynamic CI Groups**.
 2. Click **New**.
 3. On the form enter:
- | | |
|-----------------------|--------------------------|
| Name: | MyDatabases |
| Business Criticality: | 1 – most critical |
| Owned By: | David Loo |
| Operational status: | Operational |

Dynamic CI Group
New record View: New dynamic CI group*

* Name	MyDatabases
Business criticality	1 - most critical
Owned by	David Loo <input type="button" value="🔍"/>
Email	david.loo@example.com <input type="button" value="✉️"/>
Business phone	
Operational status	Operational

- In the **CMDB Group** field, select the **MyDatabases** CMDB group you just created.

Select the CMDB group to create a service based on it

CMDB Group	MyDatabases
<input type="button" value="Submit"/> <input type="button" value="View CMDB Group CIs"/>	

- Click **View CMDB Group CIs**. A new tab opens showing the 13 databases in the CMDB group.
- Close** the tab.
- Click **Submit**.
- Navigate to **Service Operations Workspace** service dashboard.

9. Observe the new **MyDatabases** tile.

The screenshot shows a dashboard with a sidebar on the left containing icons for Home, Search services, and various system status indicators. The main area displays four service tiles arranged in a 2x2 grid:

- 1 - most critical (1)**: Contains a green tile with a checkmark icon and the label "MyDatabases". This tile is highlighted with a red rectangular border.
- 2 - somewhat critical (1)**: Contains a yellow tile with an exclamation mark icon and the label "LearnNow Portal".
- 3 - less critical (1)**: Contains a green tile with a checkmark icon and the label "SurveyProject".
- 4 - not critical (1)**: Contains a green tile with a checkmark icon and the label "ServiceNow Event Management".

10. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.

11. Click **Load Sample**.

12. In the Choose Event Sample dialog box, enter **Lab2** and wait for the filtered list.

13. From the list, select **Lab2.2 DatabaseServer** and click **OK**.

source:	PSScript
node:	Lawson_db_100
message_key:	1-3DB2017
severity:	1
description:	Database not available
type:	SNDemo
source instance:	PS
additional_info:	Database Error

14. Click **Generate Event**.

15. You are redirected to All Events. **Refresh** the list until the event is **processed**.

Created on Today										
Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key	State	Severity	Alert
2022-02-09 05:36:48	PSScript	Database not available	lawson_db_100	SNDemo			1-3DB2017	Processed	Critical	Alert0010006
2022-02-09 04:30:31	PSScript	Issue on win-cls765jfqy	win-cls765jfqy	SNDemo			1-2HT2017	Processed	Major	Alert0010005
2022-02-09	PSScript	This is a Test for		SNDemo			1-1HT2017	Processed	Minor	Alert0010004

16. Open the event and observe the processing notes for CI binding.

The screenshot shows a 'Processing Notes' panel with the following text:
Binding alert CI process flow:
Node will be resolved to CI id: 60ca3062c0a8010e0145c47fe9f3dc12 found by node name
Event CI type is empty
No related CI found for binding, alert CI will be bound to node (id): 60ca3062c0a8010e0145c47fe9f3dc12
Bind to 60ca3062c0a8010e0145c47fe9f3dc12

17. To the right of the Alert field, click the **Preview this record** icon. Note the configuration item the alert was bound to.

The screenshot shows an 'Alert' details page. The 'Configuration item' field is highlighted with a blue border. A red arrow points from the text in step 17 to this highlighted field. Other fields visible include State (Processed), Alert (Alert0010007), Description (Database not available), Severity (Critical), Source (PSScript), State (Open), Maintenance, Acknowledged, and Role in Group.

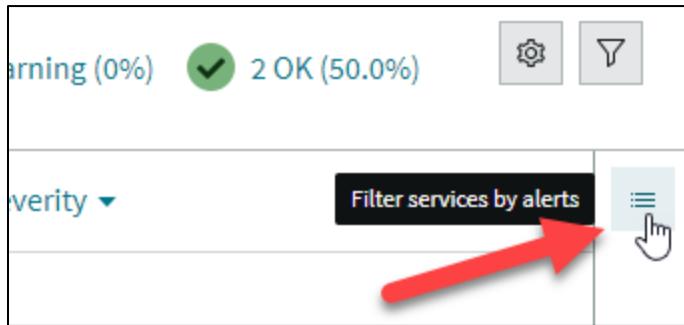
Note: The event processing engine associated the alert with the node **lawson_db_100**. This is a Unix server in the CMDB.

18. Return to the **Service Operations Workspace** service dashboard.

The screenshot shows the Service Operations Workspace dashboard. It features four service tiles: 'MyDatabases' (red, most critical), 'LearnNow Portal' (orange, somewhat critical), 'SurveyProject' (green, less critical), and 'ServiceNow Event Management' (green, not critical). A sidebar on the left includes icons for Home, Groups, and Alerts. The top navigation bar includes 'Group by Business criticality ▾', 'Group order Ascending ▾', 'Segment each group by Severity ▾', and a search bar.

Note: The **MyDatabases** tile is now red to reflect the severity of the alert. The tiles may display differently based on your browser size.

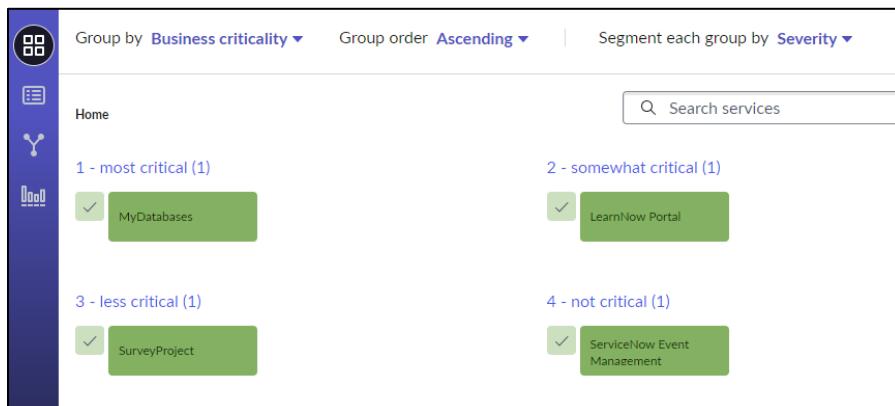
19. As a last step, clean up the Service Operations Workspace so all services are green before proceeding. Disregard any ServiceNow Event Management self-health alerts. Click the Filter services by alerts icon to display service-impacting alerts.



Alert ID	Description	Priority	Severity	Impacted Services	Last Event
Alert0010010	Database not available	Urgent	Critical	1	2022-07-12 21:17:43
Alert0010009	Issue on win-cls765jfqy	Urgent	Major	1	2022-07-12 20:32:16

Note: As in the screenshot, you should see that the MyDatabase Servers tile is red from the Critical alert we triggered earlier in this lab, and the LearnNow Portal tile is orange from the Major alert we triggered earlier. The associated alerts are listed.

- Click and open each alert in the list and click the **Close** button. The alerts open in new SOW tabs. The Close button may display as dots if the browser is not wide enough.



21. Once you have closed all open alerts on the list, your Service Operations Workspace should be completely green. Disregard any ServiceNow Event Management self-health alerts. It may take several seconds for the Service Operations Workspace to update after closing the alerts. Close the Service Operations Workspace alert tabs.



Congratulations on completing the lab!

Architecture

Execute a Discovery and Bind with IP and MAC

Lab

2.3

20m

Lab Objectives

You will achieve the following objectives:

- Run a Discovery schedule to discover your Windows Server VM
- Navigate the Discovery record
- Bind an alert to your Windows Server configuration item using the IP address
- Bind an alert to your Windows Server configuration item using the MAC address

Scenario

In this lab, you run Discovery on your Windows Server VM, which is also your MID server. Discovery creates a configuration item (CI) in the CMDB of your ServiceNow instance. You then fire two events to raise alerts bound to this Windows Server based on the value of the event node field.

A. Set Up a Discovery Schedule

1. From your ServiceNow instance, navigate to **Discovery > Discovery Schedules**.
2. Click **New**.

Note: *be patient, form display may take a few seconds*

3. Configure the **Discovery Schedule** form as follows:

Select a discovery type from the Discover list and configure its attributes.

Name	My Windows Server
Discover	Configuration items
MID Server selection method	Specific MID Server
* MID server	windows_mid <input type="button" value="🔍"/> <input type="button" value=" ⓘ"/>

4. Save.
5. From Related Links, click **Quick ranges**.

Related Links

[Quick ranges](#) (highlighted)

[Discover now](#)

[Run Point Scan](#)

6. In the dialog box enter your Windows server VM internal IP (e.g., 198.51...) identified in the previous lab and click **Make Ranges**.

Quick Ranges

Enter comma-separated IP address ranges, IP networks, or individual to add. For example:

10.0.1.0/24,10.0.2.1-10.0.2.15,10.0.3.176,10.0.3.222

Specifies an IP network with valid IP addresses between 10.0.1.1 and 10.0.1.254, an IP range from 10.0.2.1 to 10.0.2.15 inclusive, and the two individual IP addresses 10.0.3.176 and 10.0.3.222. Any entries you make that cannot be interpreted will simply be ignored.

<<your windows vm internal ip>>

Make Ranges

Cancel

Note: *The Internal IP can be found on the MID server record on the instance since this Windows server is also your MID server.*

- From Related Links, click **Discover now**.

Related Links

[Quick ranges](#)

[Discover now](#)

[Run Point Scan](#)

B. Observe the Discovery

- Open the discovery status record.
- Wait for the **State** to change to **Completed**.

Number

DIS0010033

State

Completed

Note: *This may take up to 3 minutes.*

- From the **Additional actions** menu, select **Reload form**.

- From the **Devices** related list, click the **CMDB CI** record to open the Windows server CI.

The screenshot shows the 'Devices (1)' tab selected in the 'Related Links' section. A table lists a single CMDB CI record. The 'Source' column contains 'ip-198-51-100-167'. This value is highlighted with a red box. The 'CMDB CI' column contains 'UNIX - Classify', and the 'Class' column contains 'Linux Server'.

Source	CMDB CI	Classification probe	Class
ip-198-51-100-167	UNIX - Classify		Linux Server

Note: Your Source and IP address will differ.

- From the **Network Adapters** related list, **copy** the **MAC Address**.

The screenshot shows the 'Network Adapters (1)' tab selected. A table lists a single adapter. The 'Name' column contains 'Ethernet 2', the 'IP Address' column contains '198.51.157.213', the 'Netmask' column contains '255.255.0.0', and the 'MAC Address' column contains '0E:FO:E2:F4:E8:97'. A red arrow points to the 'MAC Address' column.

Name	IP Address	Netmask	MAC Address	DHCP Enabled	Description
Ethernet 2	198.51.157.213	255.255.0.0	0E:FO:E2:F4:E8:97	true	AWS PV Network Device

Note: Your MAC Address will differ.

- Navigate to **Event Management > Simulation > Event Samples** (use your Favorites menu).
- Locate **Lab2.3 VMerror2** in the list and paste your **MAC address** into the **node** field and **save**. Be sure to remove any leading or trailing spaces.

The screenshot shows the 'Event Generators' tab selected. A table lists event samples. The 'Node' column for the row 'Lab2.3 VMerror2' is highlighted with a red box. A red arrow points to the 'Save (Enter)' button. The 'Node' field contains the MAC address '0e:82:83:fb:8f:ce'. A green checkmark icon is shown next to the save button.

Sample Name	Notes	Source	Node	Type	Resource	Source instance
Lab2.3 VMerror1	PSScript	Paste IP	SNDemo	PS		
Lab2.3 VMerror2	PSScript		0e:82:83:fb:8f:ce			

- Locate **Lab2.3 VMerror1** and type or copy/paste your private **IP address** into the **node** field and **save**.

Sample Name	Notes	Source	Node	Type	Resource
lab2.3 vMrror	Search	Search	Search	Search	Search
Lab2.3 vMrror1		PSScript	192.		
Lab2.3 VMerror2		PSScript	0e:82:83:fb:8f:ce	SNDemo	

Note: Your IP and MAC Address will differ. You now have 2 sample events, one with IP address and one with MAC address in the node field.

C. Fire Critical Event Against Your Windows Server VM CI Binding with IP Address

1. Navigate to **Event Management > Simulation > Event Generator** (use Favorite menu).
2. Click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab2** and wait for the filtered list.
4. From the list, select **Lab2.3 vMrror1** and click **OK**.

source:	PSScript
node:	{Your private IP Address } ← you entered this
in the sample	
message_key:	2-2.1WIN2017
severity:	Critical
description:	Critical service error (print spooler)
type:	SNDemo
source instance:	PS
additional_info:	{"remediation_action_resource": "Print Spooler"}

- Verify the **node** field contains your Windows VM private IP address.

Event Generator New record	
Source	PSScript
Node	192.168.1.10
Type	SNDemo

- Click **Generate Event**.
- You are redirected to All Events. **Refresh** the list until the event is **Processed**.
- Open the new event.

Events				
	Time of event	Source	Description	Node
	2023-01-24 23:42:58	PSScript	Critical service error (print spooler)	198.51.107.10

- Observe the **Processing Notes** for the event:

Processing Notes

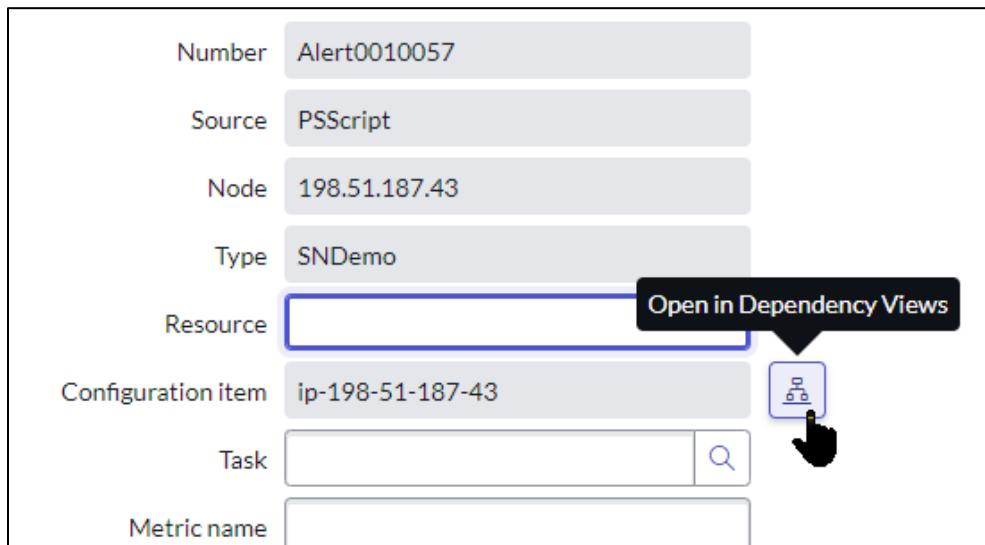
Binding alert CI process flow:
 Node is IP address
 Node will be resolved to CI id: 723f6c61f8ce23007f44536cf8b7b116 : found by IP address
 Event CI type is empty
 No related CI found for binding, alert CI will be bound to node (id): 723f6c61f8ce23007f44536cf8b7b116
 Bind to 723f6c61f8ce23007f44536cf8b7b116

Note: The event processing engine used the **Node** attribute to map the associated alert to your Windows server CI based upon a match on IP Address.

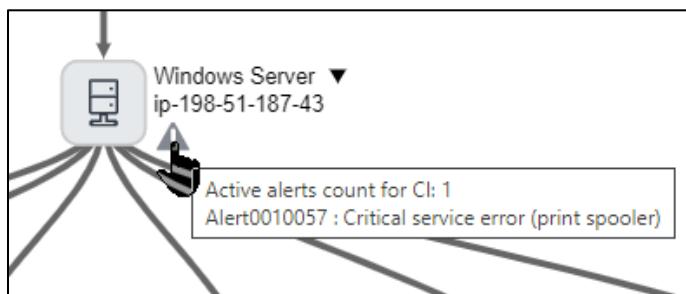
- From the Alert field of the event, **open the alert**.

Alert	
Description	Critical service error (print spooler)
Severity	Critical
State	Open
Source	PSScript
Maintenance	

11. In the alert, next to the Configuration item field, click **Open in Dependency Views** icon.



12. Hover over the exclamation point triangle on the Windows server as shown.



Note: An alert binds to your Windows server CI. Your alert number may differ.

13. **Close** the dependency view tab to return to the alert.

14. **Close** the alert.



15. From **All Alerts** (or History), **open** the alert just closed (critical service error print spooler).

16. Click **Delete**.



17. In the **Confirmation** window, click **Delete**.

D. Fire Major Event Against Your Windows Server CI Binding with MAC address

1. Navigate to **Event Management > Simulation > Event Generator**.
2. Click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab2** and wait for the filtered list.

4. From the list, select **Lab2.3 VMerror2** and click **OK**.

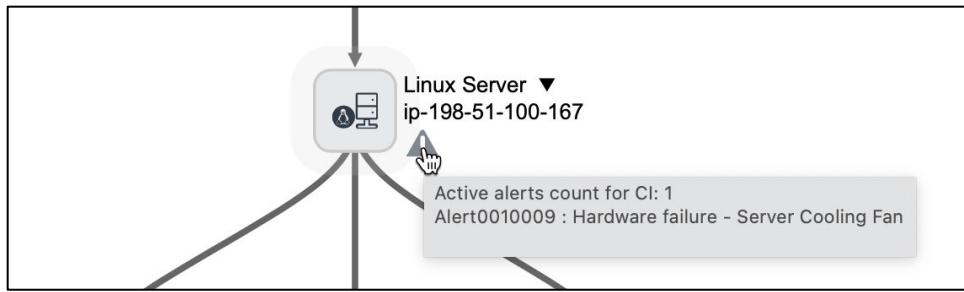
source:	PSScript
node:	{your MAC address } ← you entered this in the
sample	
message_key:	2-2.1WIN2017
severity:	Major
description:	Hardware failure - Server Cooling Fan
type:	SNDemo
source instance:	PS
additional_info:	Cooling Fan failure

5. Click **Generate Event**.
6. You are redirected to All Events. **Refresh** the list until the event state is **Processed**.
7. **Open** the new event.
8. Observe the **Processing Notes**.

```
Binding alert CI process flow:  
Node is MAC address  
Node will be resolved to CI id: b4677a14f50fd0107f442d9fe9bc9e48 : found by MAC address  
Event CI type is empty  
No related CI found for binding, alert CI will be bound to node (id): b4677a14f50fd0107f442d9fe9bc9e48  
Bind to b4677a14f50fd0107f442d9fe9bc9e48
```

9. **Open** the alert record.

10. **Open** the dependency view (e.g., ) and observe the active alert.



11. **Close** the dependency views tab.

12. **Close** the alert.

	Number	Group	Severity	Created ▾	Priority group	Priority	State	Source	Description	Node
	Search	Search	Search	2022-02-02	Search	Search	Search	Search	Search	Search
Alert0010009	Major			2022-02-02 23:53:53	High		4306 Closed	PSScript	Hardware failure - Server Cooling Fan	0e:82:83:fb:8f:ce



Congratulations on completing the lab!

Event Management

Event Processing

Lab
3.1
25m

Lab Objectives

You will achieve the following objectives:

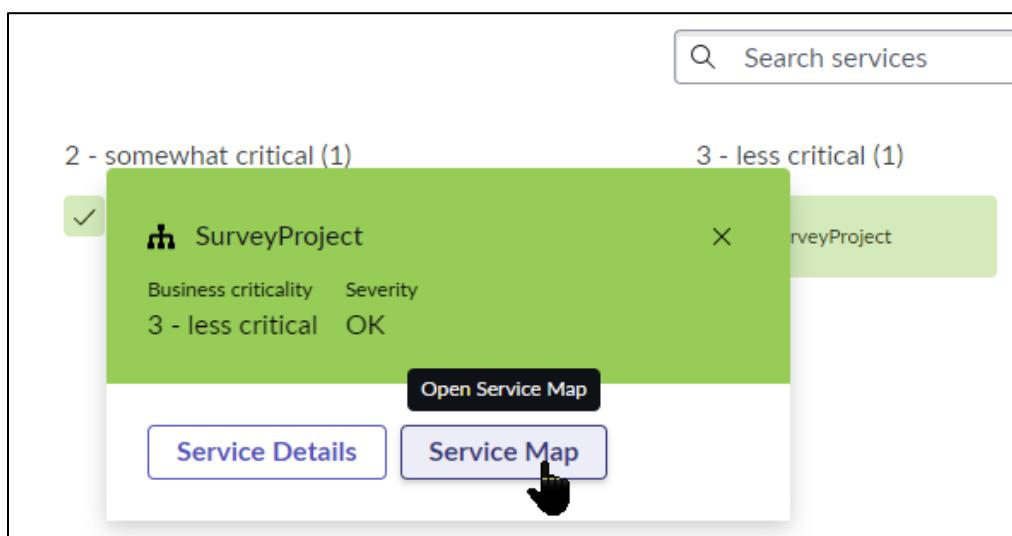
- Triggering multiple levels of events
- Binding events to services
- Manually create an incident and observe closed alert impact

Scenario

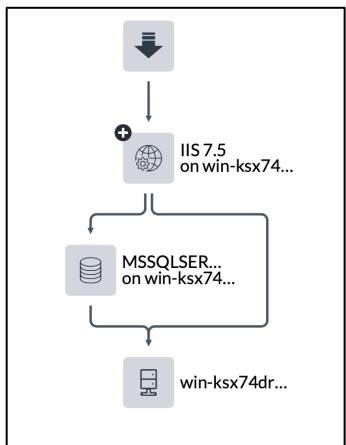
In this lab, you will use various methods to bind events to services. The baseline engine binds alerts to CIs supporting application services, creating correlated alerts.

A. Trigger a Minor Event

1. Navigate to **Service Operations Workspace** service dashboard.
2. Open the survey project **Service Map**.



3. Observe the application service map:



Note: The map displays an IIS 7.5 Web Server connected to an MSSQL Database Server. Both IIS 7.5 and MSSQLSERVER run on a host Windows Server with the name win-ksx74drkgh.

4. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
5. Click **Load Sample**.
6. In the Choose Event Sample dialog box, enter **Lab3.1** and wait for the filtered list.
7. From the list, select **Lab3.1 EventBind1** and click **OK**.

source:	PSScript
node:	win-ksx74drkgh
message_key:	3-1HT2017-SN1
severity:	Minor
description:	Server Minor Issue - Lab 3.1
type:	SNDemo

8. Click **Generate Event**.
9. You are redirected to All Events. **Refresh** the list until the event is **Processed**.
10. Open the event and observe the **Processing Notes**.

Processing Notes	<p>Binding alert CI process flow: Node will be resolved to CI id: b87413c1f8c223007f44536cf8b7b16f: found by node name Event CI type is empty No related CI found for binding, alert CI will be bound to node (id): b87413c1f8c223007f44536cf8b7b16f Bind to b87413c1f8c223007f44536cf8b7b16f</p>
------------------	---

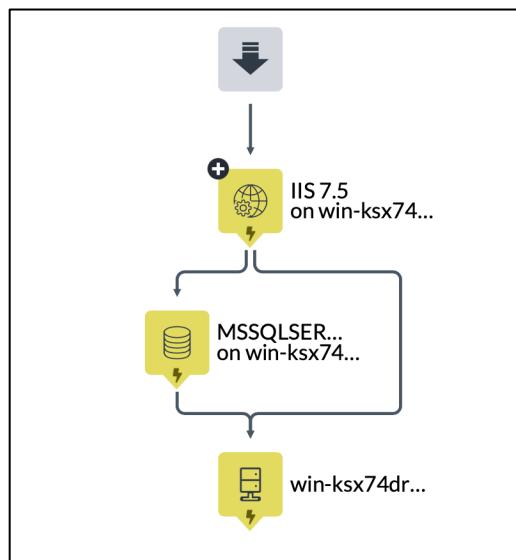
Note: The processing engine binds the alert to an existing CI based upon the node field containing an existing server name.

11. Return to the Service Operations Workspace **Survey Project** service map (hint: use History).

The screenshot shows a navigation bar with tabs: Favorites, History, Workspaces, and Admin. Below the navigation bar is a search bar labeled 'Filter'. Underneath the search bar are two entries in a list:

- Service Operations Workspace** 1 min ago
SurveyProject
- Service Operations Workspace** 1 min ago

The first entry is highlighted with a red border.



Note: The associated alert generated from the event is bound to the Windows Server `win-ksx74drkgh` and both the `IIS 7.5` and `MSSQLSERVER` CIs are affected.

12. On the right, click the **Related Items icon** to display the associated alerts.

The screenshot shows the 'Related Items' interface in ServiceNow. At the top, there's a header with a refresh button, a help icon, and a 'Related Items' icon (a circle with three horizontal lines) which is highlighted with a red box and has a red arrow pointing to it. Below the header, there are two dropdown menus: 'View' set to 'Alerts' and 'Sort by' set to 'Alert priorit...'. The main area displays a list of alerts. The first alert in the list is titled 'Server Minor Issue - Lab 3.1'. It includes columns for Priority group (High), Severity (Minor), Impacted Services (1), Configuration (win-ksx74d...), Assigned to (empty), and Assignment group (empty). At the bottom of the list, it says 'Last event : 2022-07-12 21:58:48'.

B. Trigger a Critical Event

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
2. Click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab3.1** and wait for the filtered list.
4. From the list, select **Lab3.1 EventBind2** and click **OK**.

source:	PSScript
node:	198.56.1.200
message_key:	3-1HT2017-SN2
severity:	Critical
description:	Server Critical Issue - Lab 3.1
type:	SNDemo

Note: The IP address shown in the node field of the event is the IP address of win-ksx74drkgh.

5. Click **Generate Event**.
6. You are redirected to All Events. **Refresh** the list until the event is **Processed**.
7. Open the event and observe the **Processing Notes**:

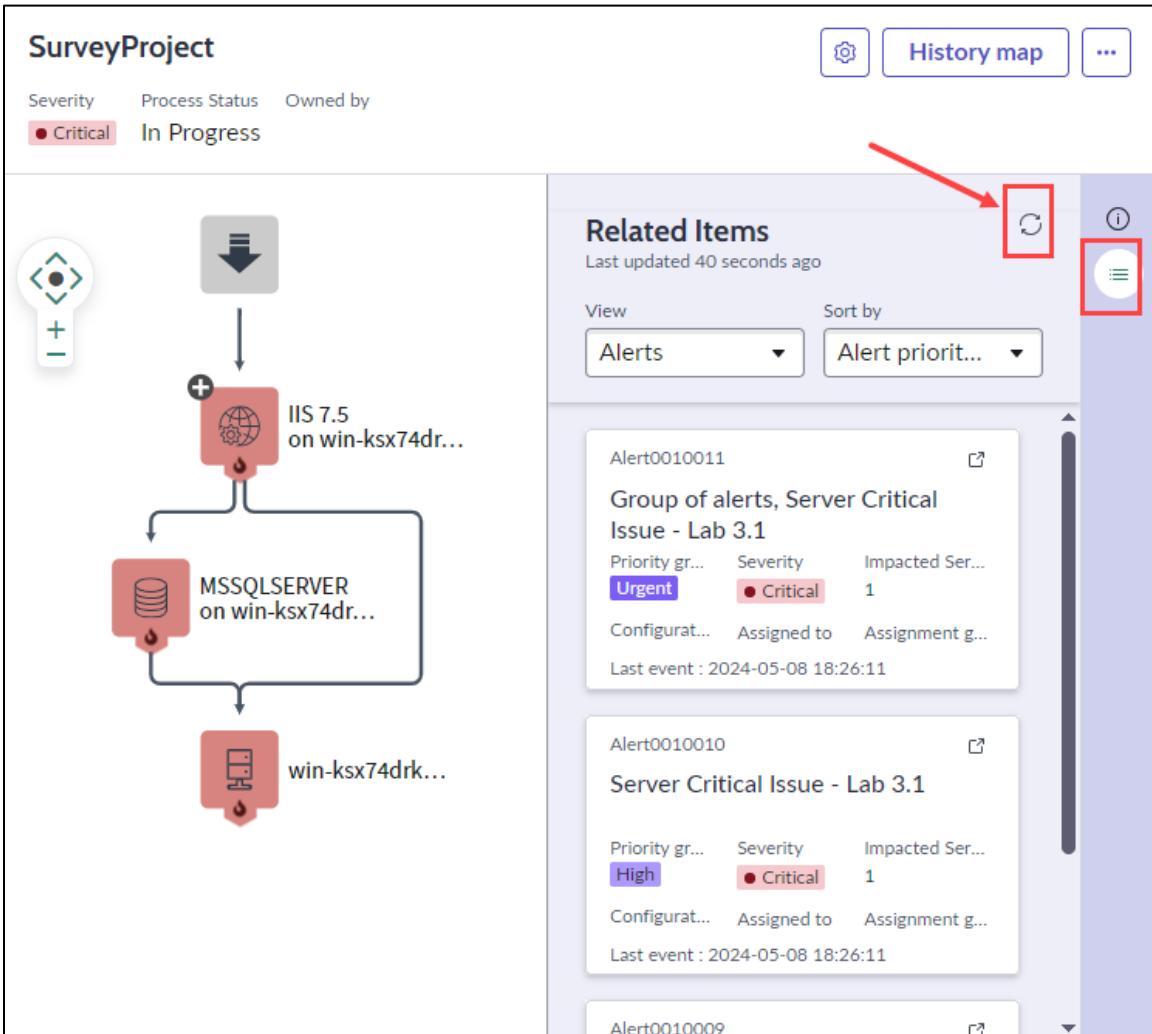
Processing Notes

Binding alert CI process flow:
Node is IP address
 Node will be resolved to CI id:c2fb8a25b17930107f442bd6e287d0d6 : found by IP address
 Event CI type is empty
 No related CI found for binding, alert CI will be bound to node (id): c2fb8a25b17930107f442bd6e287d0d6
 Bind to c2fb8a25b17930107f442bd6e287d0d6

No event rule applied
 Mapping rule(s) applied after binding: Alert Tags t_location-CMDB CI Value Based, Alert Tags t_ip_address-CMDB CI Value Based
 Not able to assign alert based on "cmdb_ci.support_group" since the "support_group" is empty
 Not able to assign alert based on the connectors assignment group ("IntegrationGroup") since it's empty

Note: The IP address in the node field is used to identify the CI for alert binding.

8. Return to Service Operations Workspace **Survey Project** service map. Display **Related Items** and refresh the list.



Note: The alert binds to win-ksx74drkgh because the event Node matches the IP address of the win-ksx74drkgh Windows Server CI in the ServiceNow CMDB. Notice in the alert list a virtual alert is created for the group of alerts.

9. Navigate to **Event Management > All Alerts**.
10. On the latest alert, click to **expand** the grouped alert and display secondary alerts. It may take a minute or two for event processing to group the alerts.

The screenshot shows a table row for an alert. The first column has a checkbox with a hand cursor icon, indicating it's expandable. The alert number is Alert0010012, severity is Critical, and priority is Low. The status is Open, and the source is Group Alert. There are search buttons for each column header.

Note: Locate the most recent “grouped” alert listed. This new virtual, primary automated alert group has been created because the critical alert and the minor alert from prior lab steps automatically group together since they bind to the same CI. Alert grouping is covered in more detail in the next module.

11. Scroll down to the **Secondary Alerts** section.

The screenshot shows a list of secondary alerts under a parent alert. Alert0010010 is a Minor alert (Severity: Minor, Priority: Low) and Alert0010011 is a Critical alert (Severity: Critical, Priority: Low). Both are grouped under Alert0010012, which is listed as the Parent. The status is Open for both. The source is PSScript. The IP address for the critical alert is 198.56.1.200.

12. Open the critical alert. Note the Parent field: the virtual alert is listed as the parent alert for this automated group.

The screenshot shows the details of the critical alert. The Parent field is set to Alert0010012. Other fields include Maintenance (unchecked), Updated (2022-02-03 00:22:33), Knowledge article (empty), and Overall Event Count (1).

13. Scroll down and view the **Impacted Services** related list.

Name	Severity	View Service	Class	Root CI Id
SurveyProject	Critical	View Service	Mapped Application Service	(empty)

14. Scroll down to the **Secondary Alerts** related list.

Number	Group	Severity	Priority group	Priority	State	Source	Description	Node	Configuration item
No records to display									

Note: The Minor alert is not listed as a Secondary alert because it is a secondary alert for the virtual grouped alert, but not this critical alert.

15. Scroll up and observe the alert has an empty Task field.

Node	198.56.1.200
Type	SNDemo
Resource	<input type="text"/>
Configuration item	win-ksx74drkgh
Task	<input type="text"/> <input type="button" value=""/>

16. At the top, click **Quick Incident**.



17. Update the incident with the following:

- Caller: **Event Management**
- Category: **Hardware**

- Assignment group: **ITSM Engineering**

The screenshot shows the ServiceNow incident creation interface. The 'Category' field is set to 'Hardware' and the 'Assignment group' field is set to 'ITSM Engineering', both of which are highlighted with red boxes. Other fields visible include 'Number' (INC0010001), 'Caller' (Event Management), 'Service offering', 'Configuration item' (win-ksx74drkg), 'Short description' (Server Critical Issue - Lab 3.1), 'Description' (Server Critical Issue - Lab 3.1), and various status and priority dropdowns.

Note: The Short Description and Configuration item populate from the alert.

- Remember the incident **Number**.

Note: Your incident Number may be different.

- Click **Update**.

C.Trigger a Clear Event

- In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
- In the upper right, click **Load Sample**.
- In the Choose Event Sample dialog box, enter **Lab3.1** and wait for the filtered list.
- From the list, select **Lab3.1 ClearEvent** and click **OK**.
- Click **Generate Event**.
- You are redirected to All Events. **Refresh** the list until the event is processed.

Note: An event is triggered with the same Message key (e.g., 3-1HT2017-SN2) as the 'Server Critical Issue' event with a severity of Clear (0). Even though the alert is part of the Alert Group, only the Critical alert closes. The associated Minor alert as well as the group alert remain open, and the severity of the group alert will be reduced to Minor.

- Navigate to **All Alerts**.

	<input type="checkbox"/>	<input type="checkbox"/>	Number	Group	Severity	Created ▾	Priority group	Priority	State	Source
▶			Alert0010012	Automated	Minor	2022-02-03 00:22:33	Moderate	2206	Open	Group Alert

Note: Note that the State of the alert remains as Open and the Severity has been reduced to Minor; it may take a few seconds for the Severity to update. Priority group value may differ.

8. **Expand** the grouped alert. Notice only the open alert is listed because of the default filter.
9. Scroll down to the **Secondary Alerts** related list and click on the “grouped” Parent alert link to remove subsequent conditions.

Secondary Alerts [1 of 5 Lists]					
Parent = Alert0010012					
	<input type="checkbox"/>	Number	Search	Search	Search
Alert0010010	<input type="checkbox"/>	Secondary	Minor	Moderate	2,206,010.001
Alert0010011	<input type="checkbox"/>	Secondary	Critical	High	2,406,010.001

Secondary Alerts [1 of 5 Lists]					
Parent = Alert0010012					
	<input type="checkbox"/>	Number	Search	Search	Search
Alert0010010	<input type="checkbox"/>	Secondary	Minor	Moderate	2,206,010.001
Alert0010011	<input type="checkbox"/>	Secondary	Critical	High	2,406,010.001

As we saw in the note above, the clear event closed the critical alert. The minor alert remains open. Priority group values may differ.

10. Open the closed **Critical** alert from the list.
11. Click the **Preview this record** icon next to the **Task** field on the alert form.

Task	INC0010001	
------	------------	--

The screenshot shows the ServiceNow Incident details page. At the top, there are fields for Configuration item (win-ksx74drkgh), Task (INC0010001), and Knowledge article. Below that is a large 'Incident' section with various fields: Number (INC0010001), Channel, State (which is highlighted with a red box and set to Resolved), Caller (Event Management), Category (Hardware), Subcategory, On hold reason, Impact (3 - Low), and a 'Resolved' button. A 'Open Record' button is also visible.

Note: Since the associated alert closed, it resolved the incident.

D. Manually Clear the Minor Alert

1. Navigate to All Alerts and expand the grouped alert.

The screenshot shows the All Alerts list. It includes search fields for Number, Group, Severity, Created, Priority group, Priority, State, and Source. Below the search bar, a grouped alert is listed with the following details: Number (Alert0010012), Group (Automated), Severity (Minor), Created (2022-02-03 00:22:33), Priority group (Moderate), Priority (2206), State (Open), and Source (Group Alert).

2. Scroll down to the Secondary Alerts related list and open the Minor alert.

The screenshot shows the Secondary Alerts related list. It includes search fields for Number and Search. Below the search bar, a secondary alert is listed with the following details: Number (Alert0010010), Secondary (Secondary), Severity (Minor), Priority group (Moderate), Priority (2,206,010.001), and State (Open). The alert is highlighted with a blue background.

3. Close the Minor alert by clicking on the Close button.

The screenshot shows the detail view of the Minor alert (Alert0010010). It includes fields for Number (Alert0010010), Source (PSScript), Node (win-ksx74drkgh), Type (SNDemo), Severity (Minor), State (Open), Acknowledged (checkbox), and Maintenance (checkbox). A 'Close' button is located at the top right of the detail view, highlighted with a red box.

Note: Manually closing the Minor alert also closes the Alert Group as this Minor alert was the last alert in the group. The automated alert could take a few moments to close.

4. Return to **Service Operations Workspace** service dashboard.

The screenshot shows the Service Operations Workspace dashboard. On the left is a sidebar with icons for Home, My Services, My Groups, and My Alerts. The main area has a search bar at the top right. The dashboard displays four service cards grouped by business criticality:

- 1 - most critical (1)**: MyDatabases (green card)
- 2 - somewhat critical (1)**: LearnNow Portal (green card)
- 3 - less critical (1)**: SurveyProject (green card)
- 4 - not critical (1)**: ServiceNow Event Management (green card)

At the bottom of the dashboard, there is a green rectangular button.

IMPORTANT NOTE: If all the services are not green, right-click on any open alerts in the All Alerts list and close them. The Service Operations Workspace needs to be completely green before proceeding. Disregard any ServiceNow Event Management self-health alerts.

Congratulations on completing the lab!

Event Management

CI Binding with Event Rules

Lab
3.2
20m

Lab Objectives

You will achieve the following objectives:

- Create event rules to populate alert fields which enables event processing to bind alerts to CIs.

Scenario

In this lab, events are fired with no automatic binding to a CI or application service because (1) the node field is empty or (2) the node and severity fields are empty. You will create event rules with regex parsing to populate those fields in the alert which will enable the correct alert to CI binding.

Discussion: There are two ways to create new event rules: from the **Create Event Rule UI** action button within an event and from the **recommended rules** link on the event rules list (see graphics below). The Next Experience UI has changed the automatic population of event rule fields from the event fields. You may need to manually create the event rule filter to match the graphic in these cases.

The left screenshot shows the ServiceNow interface with the 'Event Rules' module selected. The 'Create Event Rule' button is highlighted with a red box. The right screenshot shows a list of event rules with a red box around the header message: 'There are 21 recommended rules, created out of 83 unassociated events of the most recent 1000'.

Standard ServiceNow Event Management severities are:

- 1 – Critical
- 2 – Major
- 3 – Minor
- 4 – Warning
- 5 - OK (previously Info)
- 0 - Clear

A. Execute an Unbound Infrastructure Event

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
2. In the upper right, click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab3.2** and wait for the filtered list.
4. From the list, select **Lab3.2 UnboundEvent1** and click **OK**.

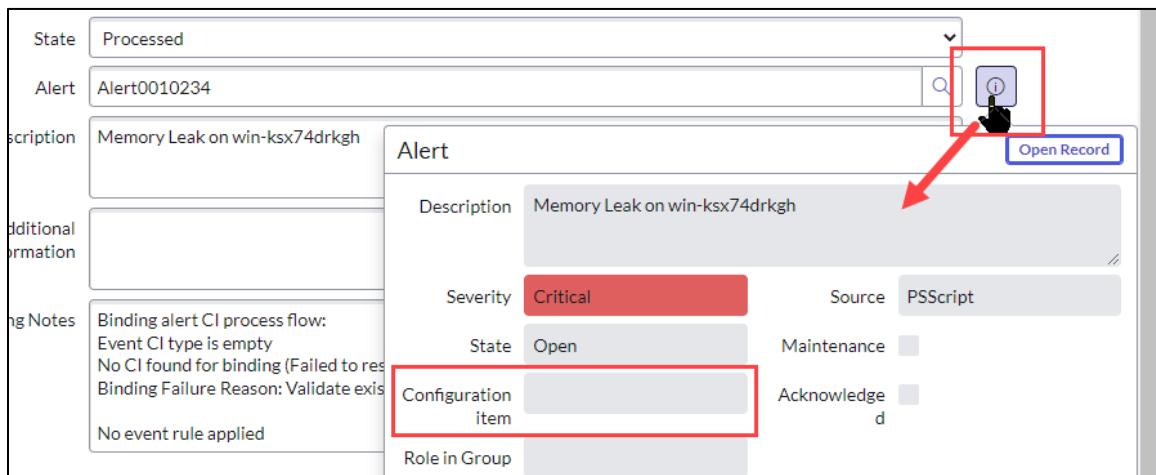
source: **PSScript**
 message_key: **3-2EX2017-SN1**
 severity: **Critical (1)**
 description: **Memory Leak on win-ksx74drkgh**
 type: **SNDemo**
 source instance: **PS**

5. Note that the **node** field is empty.
6. Click **Generate Event**.
7. You are redirected to All Events. **Refresh** the list until the event is processed.

	Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key
	Search	Search	Search	Search	Search	Search	Search	Search
2022-02-03 15:12:09	PSScript	Memory Leak on win-ksx74drkgh	SNDemo					3-2EX2017-SN1

Note: Default binding fails because the event node field is empty.

8. Open the event.
9. Next to the Alert field, click **Preview this record**.



State	Processed
Alert	Alert0010234
Description	Memory Leak on win-ksx74drkgh
Additional Information	
Notes	Binding alert CI process flow: Event CI type is empty No CI found for binding (Failed to resolve) Binding Failure Reason: Validate exists No event rule applied
Alert Description: Memory Leak on win-ksx74drkgh Severity: Critical Source: PSScript State: Open Configuration item: UnboundEvent1 (highlighted with a red box) Role in Group: Maintenance Acknowledged	

Note: The Configuration Item field in the alert is empty. The alert is unbound.

10. Click away from the preview to return focus to the event. **Review** the description and processing notes.

The screenshot shows the 'Event Details' page in ServiceNow. The 'Description' field contains the text 'Memory Leak on win-ksx74drkgh'. The 'Processing Notes' field contains the following text:
Binding alert CI process flow:
Event CI type is empty
No CI found for binding (Failed to resolve the event node to CI id)
No event rule applied
Not able to assign alert based on "cmdb_ci.support_group" since the alert is not bound to a CI
Not able to assign alert based on the connectors assignment group ("IntegrationGroup") since it's empty

Note: The Description contains the name of the server experiencing the memory leak. The Processing Notes explain no CI was found for binding.

B. Configure an Event Rule for Binding

1. Navigate to **Event Management > Rules > Event Rules**.
2. At the top of the page, click **# recommended rules**.

The screenshot shows the 'Event Rules' page in ServiceNow. The top navigation bar has 'Event Rules' selected. Below the navigation, a message states 'There are 7 recommended rules, created out of 9 unassociated events of the most recent 50000 events.' A red box highlights the link '7 recommended rules'.

Note: Your number of recommended rules may differ.

3. Locate and expand the recommended event group for this event, **Memory Leak on win-ksx74drkgh**.

The screenshot shows the expanded 'Event group: PSScript: Memory Leak on win-ksx74drkgh (1)' in the list. The expanded view shows the following details:
Event group: PSScript: Database not available (1)
Event group: PSScript: Hardware failure - Server Cooling Fan (1)
Event group: PSScript: Memory Leak on win-ksx74drkgh (1)
Memory Leak on win-ksx74drkgh
Event group: PSScript: Server (*) Issue (*) - Lab (*) (3)

4. Click the recommended rule.

A screenshot of a software interface showing a list of event groups. The first item is 'Event group: PSScript: Memory Leak on win-ksx74drkgh (1)'. Below it is 'Memory Leak on win-ksx74drkgh'. A red arrow points to this item, and a hand cursor icon is positioned over it. To the right of the list, the text 'Memory Leak on win' is visible. Below the main list is another item: 'Event group: PSScript: Server (*) Issue (*) - Lab (*) (3)'.

5. On the Event Rule Info tab, enter:

Name - **Memory Leak Server Binding - Lab 3.2**
Source - **PSScript**

A screenshot of the 'Event Rule Info' tab. It contains the following fields:

- * Name: Memory Leak Server Binding - Lab 3.2
- Source: PSScript
- * Order: 100
- Description: (empty)

6. Click **Event Filter**.



Note: The event rule may or may not have a pre-configured filter.

7. **Modify** the filter conditions as shown below. The order of the conditions does not matter. Modify the description to use **starts with**.

All of these conditions must be met

Type	is	SNDemo
Severity	is	Critical
AND		
Source instance	is	PS
Classification	is	IT
Description	starts with	Memory Leak

8. Click **Transform and Compose Alert Output**.



9. Click on the **Description** attribute in the **Event Raw Info** section on the right of the form to open the Edit Regex Expressions form.

Event Input

Description
Event Raw Info

Description	Memory Leak on win-ksx74drkgh
Node	

10. Standard edit mode is selected by default.



11. Left-click, drag, and highlight the server name.

12. Select **Node**.

13. Click to select **regex mode </>**.

Note: The highlighted string is mapped to the **Node** attribute.

14. Observe the regular expression automatically created.

Note: Rather than looking for the string **win-ksx74drkgh**, the regex searches for an unlimited string of any characters after '**Memory Leak on**' in the **Description** field, then that string is mapped to the **Node** attribute of the alert.

15. Click **Done**.



Note: *The node attribute is already the default in the Alert Node field .If it was not, you would add it.*

16. Click **Submit** to complete the event rule.



C.Test the Event Rule

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
2. In the upper right, click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab3.2** and wait for the filtered list.
4. From the list, again select **Lab3.2 UnboundEvent1** and click **OK**.
5. Click **Generate Event**.
6. You are redirected to All Events. **Refresh** the list until the event is processed.
7. **Open** the new event and observe the Processing Notes.

Processing Notes

Binding alert CI process flow:
 Node will be resolved to CI id: c2fb8a25b17930107f442bd6e287d0d6 found by node name
 Event CI type is empty
 No related CI found for binding, alert CI will be bound to node (id): c2fb8a25b17930107f442bd6e287d0d6
 Bind to c2fb8a25b17930107f442bd6e287d0d6

Event rule applied: Memory Leak Server Binding - Lab 3.2
 Mapping rule(s) applied after binding: Alert Tags t_location-CMDB CI Value Based, Alert Tags t_ip_address-CMDB CI Value Based

Note: *The event rule is applied and recorded in the Processing Notes.*

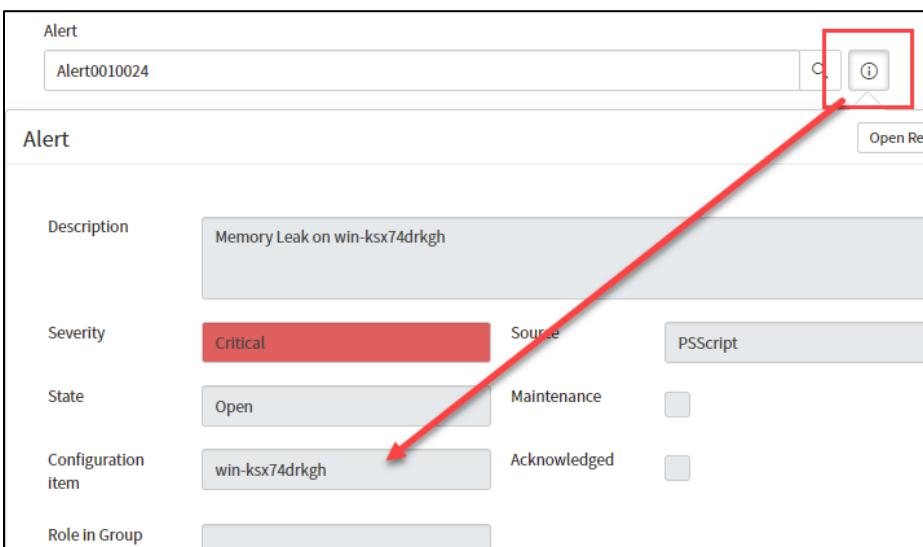
8. Under **Related Links**, click **Find matching rules**.

(i) The following list contains the matching event rules without assignment group which will be executed:
[Memory Leak Server Binding - Lab 3.2](#)
 No rules with assignment group null will be applied. Could not find any rules that match the event.

The following rules without assignment group match the event's source but their filter condition does not match this event:
[APE - Promote Event](#)

Note: *A message displays listing matching event rules.*

9. Click the **Preview this Record** icon to preview the alert. Notice the alert CI binding to the server CI.

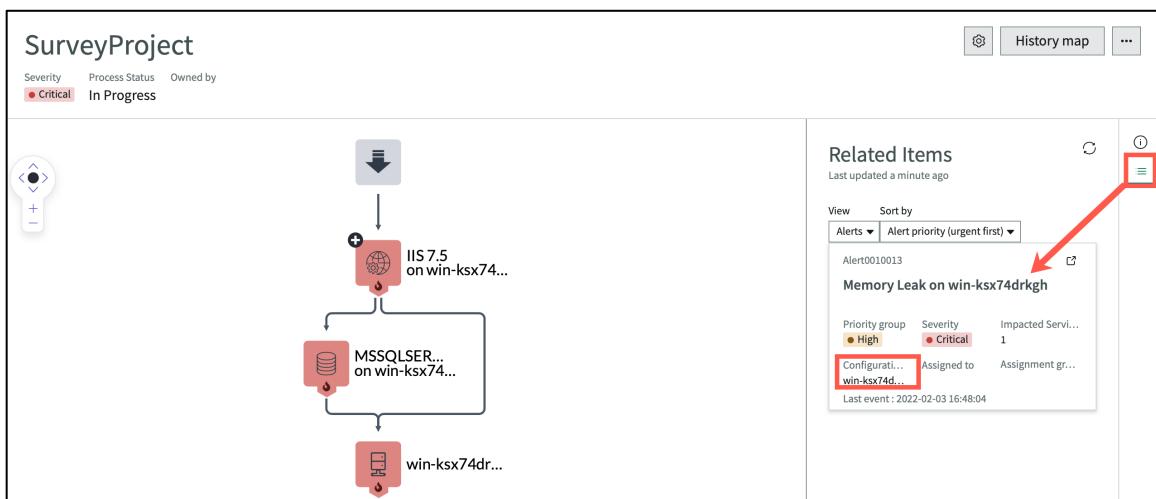
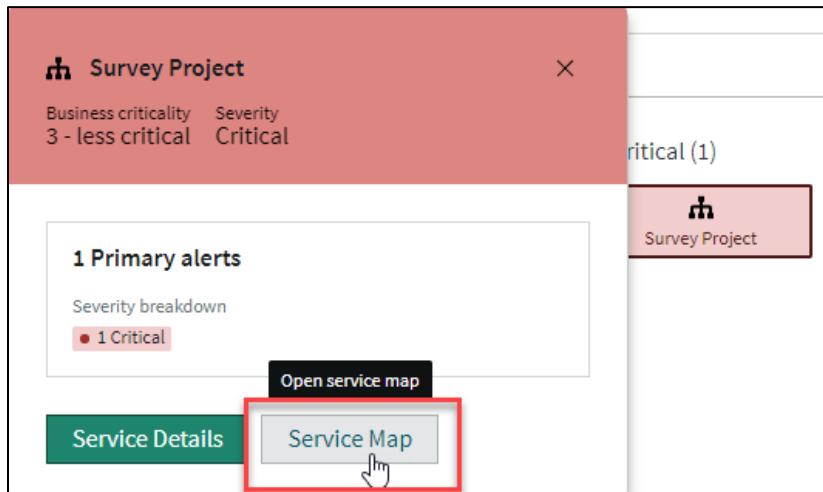


The screenshot shows the 'Alert' record page. At the top, there is a header with the title 'Alert' and a sub-header with the ID 'Alert0010024'. To the right of the sub-header are two icons: a magnifying glass and a person icon, both enclosed in a red box. Below the header, there is a table with several fields:

Description	Memory Leak on win-ksx74drkgh		
Severity	Critical	Source	PSScript
State	Open	Maintenance	<input type="checkbox"/>
Configuration Item	win-ksx74drkgh	Acknowledged	<input type="checkbox"/>
Role in Group			

A red arrow points from the text 'Notice the alert CI binding to the server CI.' to the 'Configuration Item' field, which contains the value 'win-ksx74drkgh'.

10. Return to **Service Operations Workspace** and open the **Survey Project service map**.



Note: An alert is mapped to the win-ksx74drkgh Windows server CI and is affecting the IIS 7.5 and MSSQLSERVER CIs.

11. Open the alert and review the configuration item server binding.

The screenshot shows the 'Overview' tab selected in the top navigation bar. Below it, the 'Summary' section is expanded. Under 'Identified issue', there is a 'Description' field containing 'Memory Leak on win-ksx74drkgh'. In the 'Impact' section, a 'Configuration item' box is highlighted with a red border. Inside this box, there are two fields: 'Name' with the value 'win-ksx74drkgh' and 'Class' with the value 'Windows Server'.

12. Select Close.



D. Process an Event Without a Node or Severity

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
2. In the upper right, click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab3.2** and wait for the filtered list.
4. From the list, select **Lab3.2 UnboundEvent2** and click **OK**.

```
source:          PSScript
message_key:    3-2EX2017-SN2
description:    Error on 198.56.1.200 I/O disk read operation error
type:           SNDemo
source instance: PS
additional_info: "{status:'3'}
```

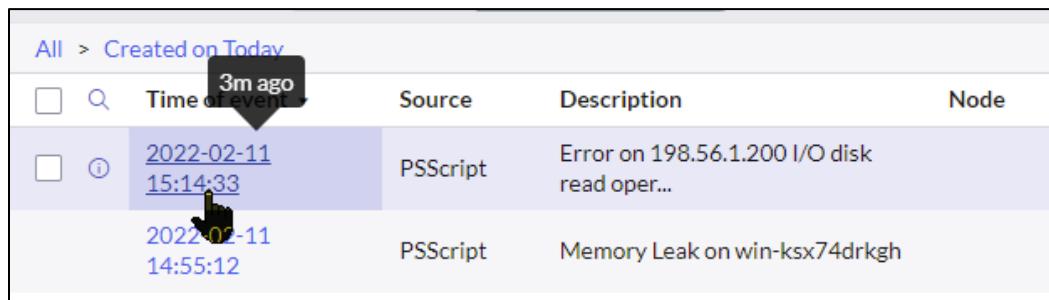
- Note that this event has no **node** or **severity** and that **additional info** is a name-value pair. Name-value pairs are captured by event processing and available for use in event rules.
- Click **Generate Event**.
- You are redirected to All Events. **Refresh** the list until the event is processed.
- Locate the event. Notice the **State** field (Error).



Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key	State
Search	Search	Search	Search	Search	Search	Search	Search	Search
2022-02-03 16:58:16	PSScript	Error on 198.56.1.200 I/O disk read oper...	SNDemo				3-2EX2017-SN2	Error

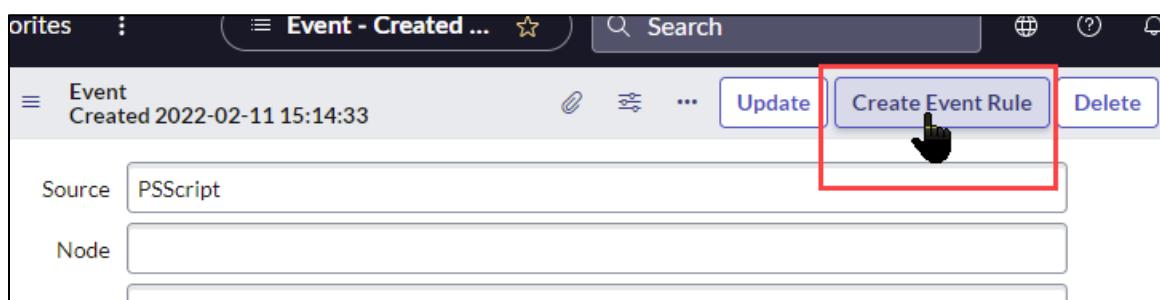
Note: *The event is unbound because there is no Node. No alert generates because there is no severity. It may take a few seconds for the State to update to Error.*

- Open the event by clicking the **timestamp**.



All > Created on Today	Time of event	Source	Description	Node
<input type="checkbox"/> 3m ago	2022-02-11 15:14:33	PSScript	Error on 198.56.1.200 I/O disk read oper...	
<input type="checkbox"/>	2022-02-11 14:55:12	PSScript	Memory Leak on win-ksx74drkgh	

- Click **Create Event Rule**.



Event	Created 2022-02-11 15:14:33	Update	Create Event Rule	Delete
Source	PSScript			
Node				

- Name the event rule: **Disk read error - Lab 3.2**.

The screenshot shows the 'Event Rule Info' section of a configuration interface. At the top, there are tabs for 'Event Rule Info' and 'Event Filter'. Below the tabs, the 'Event Rule Info' section contains the following fields:

- Name:** Disk read error - Lab 3.2
- Source:** PSScript
- Order:** 100

12. Click **Event Filter** at the top.

13. Modify the filter as:

- **Description** | contains | I/O disk read (AND)
- **Type** | is | SNDemo (AND)
- **Source Instance** | is | PS (AND)
- **Classification** | is | IT

14. If preset, remove the **status** condition.

The screenshot shows the 'Event Filter' configuration interface. A condition for 'status' is listed, which is being removed. The condition is set to 'is' with value '3'. To the right, there are buttons for 'Remove this condition' (with a delete icon), 'OR', and 'AND'.

15. Ensure your conditions match as shown:

The screenshot shows the 'Event Filter' configuration interface with four conditions defined under 'All of these conditions must be met':

- Description** | contains | I/O disk read
- Type** | is | SNDemo
- Source instance** | is | PS
- Classification** | is | IT

A blue bracket on the left indicates that the first four conditions are grouped by 'AND'.

Note: *The purpose of modifying these conditions is to enable the rule to apply to any host and any status value for this type of I/O disk read error.*

16. Click **Transform and Compose Alert Output** at the top.

17. Click the **Description** attribute in **Event Raw Info**.

The screenshot shows the 'Event Raw Info' panel. At the top, it says 'Event Raw Info'. Below that, there are two columns: 'Description' and 'Error on 198.56.1.200 I/O disk read operation error'. The 'Description' column is highlighted with a red rectangular border.

18. Highlight the IP address and bind to **Node**.

The screenshot shows the 'Expressions' panel. On the left, under 'Mark Expressions', there is a line of text: 'Error on 198.56.1.200 I/O disk read operation error'. To the right, under 'Expressions', there is a row with a blue button labeled 'Node X'.

19. Click **Done**.

20. Under **Event Additional Info**, click **status**.

The screenshot shows the 'Event Additional Info' panel. At the top, it says 'Event Additional Info'. Below that, there are two columns: 'status' and '3'. The 'status' column is highlighted with a red rectangular border.

21. Highlight the status value and bind to **Severity**.

The screenshot shows the 'Expressions' panel. On the left, under 'Mark Expressions', there is a line of text: '3'. To the right, under 'Expressions', there is a row with a blue button labeled 'Severity X'.

22. Click **Done**.

23. Observe the **Expressions** in the event rule and how this regex extracted data will be populated into the alert.

Transform and Compose Alert Output

Compose Alert fields by adding free text and by dragging variables from the right pane.
Click Event Raw values to create new regex expressions.

Description	<code> \${description}</code>
Node	<code> \${node}</code> ←
Type	<code> \${type}</code>
Resource	<code> \${resource}</code>
Message key	<code> \${message_key}</code>
Severity	<code> \${severity}</code> ←
Metric name	<code> \${metric_name}</code>

Event Input

Event Additional Info

status	3
--------	---

Expressions

Node	198.56.1.200
Severity	3

Event Raw Info

Description	Error on 198.56.1.2
Node	

24. Click **Submit** to complete the event rule.

E. Test the Event Rule

1. Trigger the event **Lab3.2 UnboundEvent2** once more.
2. Find the event and observe the event **Processing Notes**.

Processing Notes

Binding alert CI process flow:
Node is IP address ←

Node will be resolved to CI id: c2fb8a25b17930107f442bd6e287d0d6; found by IP address

Event CI type is empty

No related CI found for binding, alert CI will be bound to node (id): c2fb8a25b17930107f442bd6e287d0d6

Bind to c2fb8a25b17930107f442bd6e287d0d6

Event rule applied: Disk read error - Lab 3.2

Mapping rule(s) applied after binding: Alert Tags t_location-CMDB CI Value Based, Alert Tags t_ip_address-CMDB CI Value Based

Not able to assign alert based on "cmdb_ci.support_group" since the "support_group" is empty

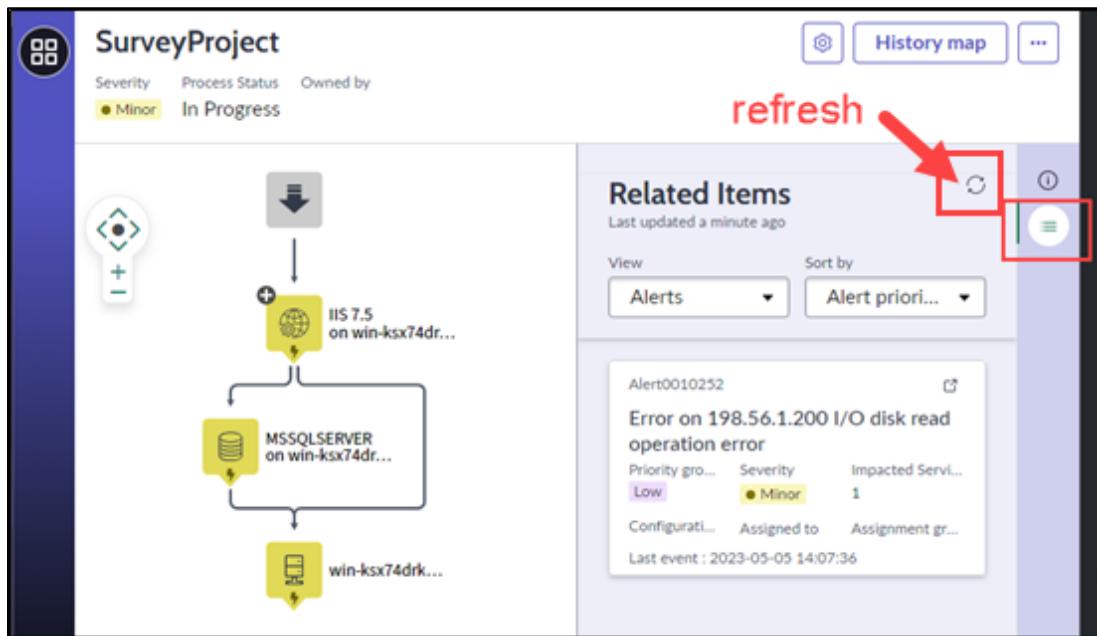
Not able to assign alert based on the connectors assignment group ("IntegrationGroup") since it's empty

3. Preview the Alert. Notice the severity = minor (3) and CI = server CI.

The screenshot shows the 'Alert' details page. At the top, there's a search bar with 'Alert0010025' and a magnifying glass icon. Below it, the alert ID 'Alert0010025' is displayed. The main area contains the following fields:

- Description:** Error on 198.56.1.200 I/O disk read operation error
- Severity:** Minor (highlighted with a red box)
- Source:** PSScript
- State:** Open
- Maintenance:** (checkbox)
- Configuration item:** win-ksx74drkgh (highlighted with a red box)
- Acknowledged:** (checkbox)

4. Return to the **Service Operations Workspace** service map for **Survey Project** and refresh the alert list.



Note: The Severity of the alert is mapped based upon the status value from the event by the newly created event rule. Priority group value may vary.

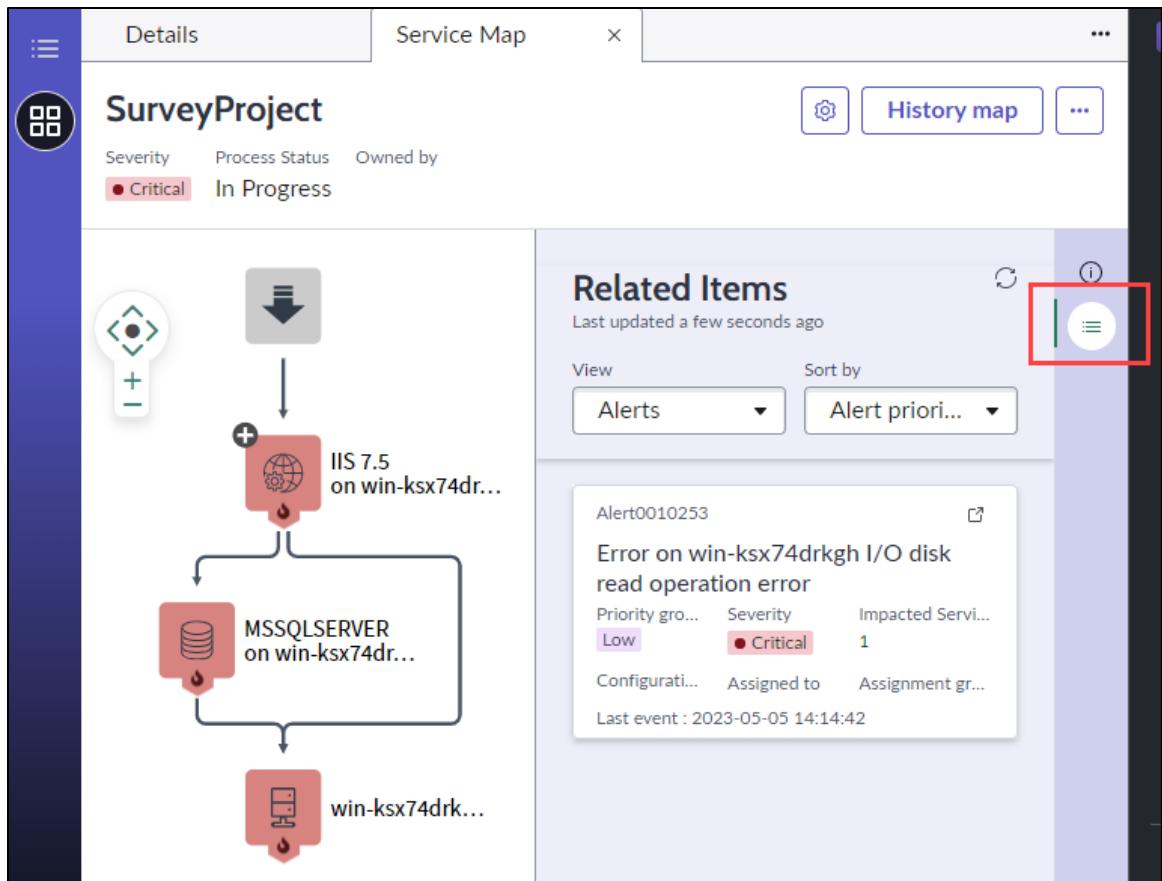
5. Close the alert.

Lab Verification

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
2. In the upper right, click **Load Sample**.
3. In the Choose Event Sample dialog box, enter **Lab3.2** and wait for the filtered list.
4. From the list, select **Lab3.2 UnboundEvent3** and click **OK**.

```
source:          PSScript
message_key:    3-2EX2017-SN3
description:    Error on win-ksx74drkgh I/O disk read operation error
type:           SNDemo
source instance: PS
additional_info: {"status": "1"}
```

5. Click **Generate Event**.
6. You are redirected to All Events. **Refresh** the list until the event is processed.
7. **Return** to the Survey Project service map.



Note: This alert binds to the win-ksx74drkgh Windows server CI based on the node extracted from the event Description. The Severity is Critical based on the status of 1 in the event Additional Info. Priority group may vary.

8. Close the Alert.

Note: Alert aggregation group alerts bind to the same CI if they are created within 10 minutes of each other, so the last two alerts in this lab may have a parent alert automatically created. In this case, then both alerts become secondary (like what occurred toward the end of lab 3.1), because they are generated within minutes of each other. Note that this is dependent upon on the speed at which you complete the labs. If this does occur, then technically you are closing a group alert here and not the actual alert from the event. It will look the same, except the source is Group Alert.



Congratulations on completing the lab!

Event Management

Event Rule Thresholds

Lab
3.3
40m

Lab Objectives

You will achieve the following objectives:

- Process events based on threshold values

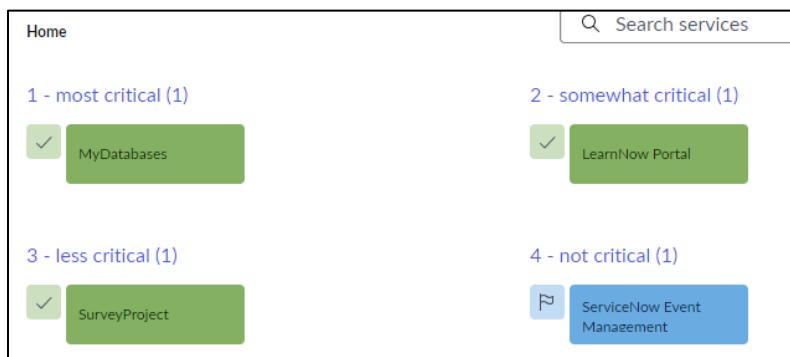
 **Lab Dependency:** Requires the completion of Lab 3.2.

Scenario

In this lab, you process events based on threshold values. An alert is generated from a threshold configured based on a percentage in the event. If the threshold is not met, no alert is generated.

A. Execute a CPU Event

- Close all open alerts. The Service Operations Workspace service dashboard should be all green. Disregard any ServiceNow Event Management self-health alerts.



- In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
- In the upper right, click **Load Sample**.
- In the Choose Event Sample dialog box, enter **Lab3.3** and wait for the filtered list.
- From the list, select **Lab3.3 CPUUsage1** and click **OK**.

```

source:      PSScript
message_key: 3-5EX2017-SN1
node:        198.56.1.200
severity:    Major (2)
description: CPU running above 70% capacity
type:        SNDemo
source instance: PS

```

6. Click **Generate Event**.
7. You are redirected to All Events. **Refresh** the list until the event is processed. Notice an alert is generated.
8. Locate the alert.

The screenshot shows two windows side-by-side. On the left is the 'Events' list window, which has a header with 'Events', 'Time of event', and 'Search'. It displays a single event row: '2023-05-05 14:28:00' (Time of event), 'PSScript' (Source), and 'CPU running above 70% capacity' (Description). On the right is the 'Alert' details view, which has a header with 'Actions on selected rows...', 'New', 'State', 'Severity', and 'Alert'. It shows one alert entry: 'Processed' (State), 'Major' (Severity), and 'Alert0010254' (Alert ID). A red arrow points from the 'Alert' column in the Events list to the 'Alert' field in the Alert details view, indicating the relationship between the event and the generated alert.

Note: An alert generates with a severity of Major.

9. **Open** the alert.
10. Click **Close**.
11. **Open** the alert again.
12. Click **Delete**.
13. Click **Delete** in the confirmation window. We are deleting the alert so that it is not “reopened” by subsequent events.

B. Create an Event Rule with Threshold

In this section, we want to generate a Major alert only if the CPU usage percentage exceeds 90% (i.e., a threshold). Note that the CPU percentage is embedded in the Description field, so we will use regex to extract the value.

1. Navigate to **Event Management > Rules > Event Rules**

2. Using the **recommended rules** link, configure the appropriate event rule with name: **CPU Threshold - Lab 3.3**.

Note: Start with the rule labeled, "CPU running above 70% capacity".

A screenshot of a software interface showing a list of event groups. The first item is a general note about impact jobs. The second item is a rule named 'CPU running above 70% capacity' (1). A red box highlights the checkbox next to this rule, and a red arrow points to the rule's name. A cursor is hovering over the rule's name. The third item is another rule related to PSScript and critical service errors.

- ▶ Event group: EMSelfMonitoring: There is delay in the impact jobs. The longest delay is (*) seconds. Additional details can be found in the log file.
- Event group: PSScript: CPU running above 70% capacity (1)
CPU running above 70% capacity
- ▶ Event group: PSScript: Critical service error (print spooler) (1)

A screenshot of the 'Event Rule Info' configuration page. It shows three fields: Name (CPU Threshold - Lab 3.3), Source (PSScript), and Order (100).

Event Rule Info		
* Name	CPU Threshold - Lab 3.3	
Source	PSScript	
* Order	100	

3. Configure the **Event Filter** section as shown:

A screenshot of the 'Event Filter' configuration page. It shows a logical 'AND' condition with four filter criteria:
1. Description contains 'CPU running above'
2. Type is 'SNDemo'
3. Source instance is 'PS'
4. Classification is 'IT'

All of these conditions must be met

All of these conditions must be met		
Description	contains	CPU running above
Type	is	SNDemo
Source instance	is	PS
Classification	is	IT

4. From the **Transform and Compose Alert Output** section, click on the **Description** attribute on the right:

Event Raw Info

Description	CPU running above 70% capacity
-------------	--------------------------------

5. Left-click, drag, and highlight the value **70**. Do not include the percent symbol.
6. Enter a field name of **cpu** and then from your keypad hit **enter** (type in **cpu** and hit **ENTER**).

Mark Expressions

CPU running above 70% capacity

cpu

7. From the top right of the form, click **</>** to enter regex mode.
8. Observe the regular expression created.

Original field is: Description
Mark or edit string to turn it into a regex expression under Transform Data

Write Regex

CPU running above (.*)% capacity

Expressions

cpu

Note: The **(.*)** regex picks up any value before the **%** and after **above** to populate in the **cpu** attribute.

9. Click **Done**.
10. Configure the **Threshold** section as shown:

• Active:	checked
• Create Alert Operator:	> (greater than)
• Field name:	cpu
• Threshold value:	90
• Occurs:	3
• Over (seconds):	60
• Close Alert Operator:	Idle
• Over (seconds):	120

Threshold

Select to create alerts only when the incoming matching events pass over the specified threshold. Once selected, other related values can be specified.

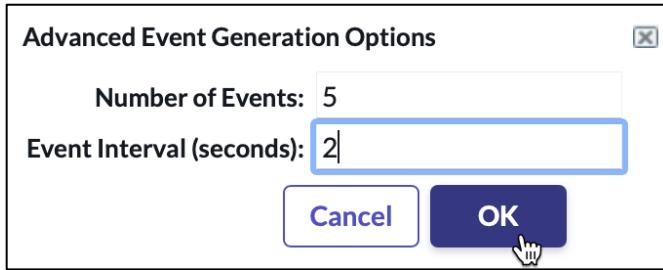
<input checked="" type="checkbox"/> Active	Ev
Create Alert Operator >	Ex
* Field name cpu	cpu
* Threshold value 90	Eve
* Occurs 3	De
* Over(seconds) 60	No
Close Alert Operator Idle	Type
* Over(seconds) 120	Re
	Me

Note: This threshold suppresses the generation of alerts unless more than 3 events occur within 60 seconds and the value of cpu is > 90. The alert closed when no further events occur for 120 seconds.

11. Click **Submit**.

C.Test the Threshold Event Rule using Advanced Event Generator

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**. The last sample event (**Lab3.3 CPUUsage1**) should still be loaded.
2. In the upper right, click **Advanced Generator**.
3. In the advanced generator options window, enter **5 and 2** to fire the event five times in two second intervals.



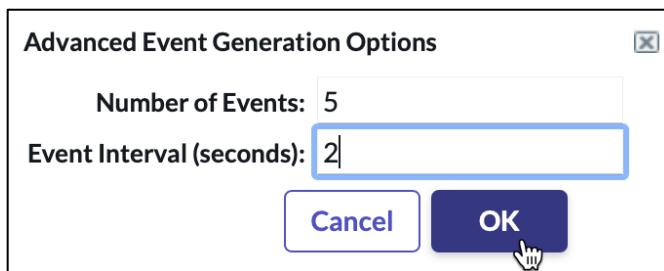
4. Click **OK**. This generates a sequence of CPU usage events (one event every 2 seconds, five times).
5. You are redirected to All Events. **Refresh** the list until all 5 events are processed.

Description	Node	Type	Resource	Metric Name	Message key	State	Severity	Alert
Search	Search	Search	Search	Search	Search	Search	Search	Search
CPU running above 70% capacity	198.56.1.200	SNDemo		3-5EX2017-SN1	Processed	Major	(empty)	
CPU running above 70% capacity	198.56.1.200	SNDemo		3-5EX2017-SN1	Processed	Major	(empty)	
CPU running above 70% capacity	198.56.1.200	SNDemo		3-5EX2017-SN1	Processed	Major	(empty)	
CPU running above 70% capacity	198.56.1.200	SNDemo		3-5EX2017-SN1	Processed	Major	(empty)	
CPU running above 70% capacity	198.56.1.200	SNDemo		3-5EX2017-SN1	Processed	Major	(empty)	
CPU running above 70% capacity	198.56.1.200	SNDemo		3-5EX2017-SN1	Processed	Major	(empty)	

Discussion: Why is no alert generated when 5 Major events are created within approximately 10 seconds?

Note: Review the earlier configuration in the previous section for the answer.

6. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
7. In the upper right, click **Load Sample**.
8. In the Choose Event Sample dialog box, enter **Lab3.3** and wait for the filtered list.
9. From the list, select **Lab3.3 CPUUsage3** and click **OK** (we are not using CPUUsage2). Read the event description!
10. In the upper right, click **Advanced Generator**.
11. In the advanced generator options window, **enter 5 and 2** to fire the event five times in two second intervals.



12. Click **OK**. This generates a sequence of CPU usage events.
13. Observe the same number of events execute but this time a related alert is generated.

Description	Node	Type	Resource	Metric Name	Message key	State	Severity	Alert
Search	Search	Search	Search	Search	Search	Search	Search	Search
CPU running above 91% capacity	198.56.1.200	SNDemo			3-5EX2016-SN3	Processed	Major	Alert0010025
CPU running above 91% capacity	198.56.1.200	SNDemo			3-5EX2016-SN3	Processed	Major	Alert0010025
CPU running above 91% capacity	198.56.1.200	SNDemo			3-5EX2016-SN3	Processed	Major	Alert0010025
CPU running above 91% capacity	198.56.1.200	SNDemo			3-5EX2016-SN3	Processed	Major	Alert0010025
CPU running above 91% capacity	198.56.1.200	SNDemo			3-5EX2016-SN3	Processed	Major	Alert0010025

Note: The Event Management Service Operations Workspace will also reflect a major alert on the Survey Project service.

14. Wait two minutes, then open the alert.

Question: Why is the alert closed when all these Major events have been generated triggering the alert?

Note: Review the earlier configuration in the previous section for an explanation on the alert's closure.

Challenge Task: Create Custom Threshold

1. Fire the **Lab3.3Diskspace1** event

source: **PSScript**
message key: **3-5EX2017-SN4**

severity: **Major (2)**
 description: **Disk space less than 1000MB**
 type: **SNDemo**
 source instance: **PS**

2. Set up an appropriate event rule extracting the disk space value for a threshold. An alert should only generate if the disk space falls below **700MB**. The alert should close if no further event is generated for **3 minutes**.
3. Test the new event rule by deleting the previously generated alert and firing both the **Lab3.3 Diskspace1** (see above) and the **Lab3.3 Diskspace2** (below) events:

source: **PSScript**
 message key: **3-5EX2017-SN5**
 severity: **2**
 description: **Disk space less than 600MB**
 type: **SNDemo**
 source instance: **PS**

Note: An alert should only generate on the second event.

Possible Solution

All of these conditions must be met					
AND	Description	contains	Disk space less than	OR	AND
	Type	is	SNDemo	OR	AND
	Source instance	is	PS	OR	AND
	Classification	is	IT	OR	AND

Edit Regex Expressions	
Original field is: Description Mark or edit string to turn it into a regex expression under Transform Data	
Write Regex Disk space less than (.*)MB	Expressions disk_space

Threshold

Select to create alerts only when the incoming matching events pass over the specified threshold. Once selected, other related values can be specified.

Active

Create Alert Operator < ▾

* Field name disk_space

* Threshold value 700

* Occurs 1

* Over(seconds) 120

Close Alert Operator Idle

* Over(seconds) 180

Description	Node	Type	Resource	Metric Name	Message key	State	Severity	Alert
Disk space less than 600MB	Search	Search	Search	Search	Search	Search	Search	Search
Disk space less than 1000MB	SNDemo	SNDemo	3-5EX2017-SN5	Processed	Major	Alert0010028	(empty)	

Congratulations on completing the lab!

Event Management

Event Binding with Event Rules and CI Field Matching

Lab
3.4
35m

Lab Objectives

You will achieve the following objective:

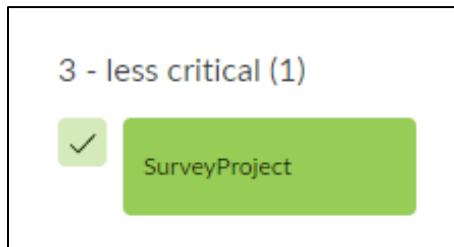
- Bind alerts using event rules and CI Field Matching

Scenario

In this lab, you fire an event that binds an alert to the host (server) CI when binding to the application CI (IIS web server) is more appropriate. You will use event rules and CI field matching to correctly configure binding of an alert to an IIS web server application CI within the Survey Project application service.

A. Execute an Unbound Infrastructure Event

1. Navigate to **Service Operations Workspace** and **close** all alerts associated with Survey Project. Ensure the service is showing green on the Service Operations Workspace.



2. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
3. In the upper right, click **Load Sample**.
4. In the Choose Event Sample dialog box, enter **Lab3.4** and wait for the filtered list.
5. From the list, select **Lab3.4 UnboundEvent-IIS** and click **OK**.

source: PSScript
message_key: 3-3X2017-SN1

node: **win-ksx74drkgh**
 severity: **Minor (3)**
 resource: **hosted application**
 description: **IIS Server locked error 423; IIS 7.5**
 type: **SNDemo**
 source instance: **PS**
 additional_info: **{'version':'7.5'}**

6. Click **Generate Event**.

7. You are redirected to All Events. **Refresh** the list until the event is processed.

8. **Locate** the event.

	Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key
	Search	Search	Search	Search	Search	Search	Search	Search
	2022-02-04 15:43:30	PSScript	IIS Server locked error 423; IIS 7.5	win-ksx74drkgh	SNDemo	hosted application		3-3EX2017-SN1

Note: The event has a Node referring to the host CI.

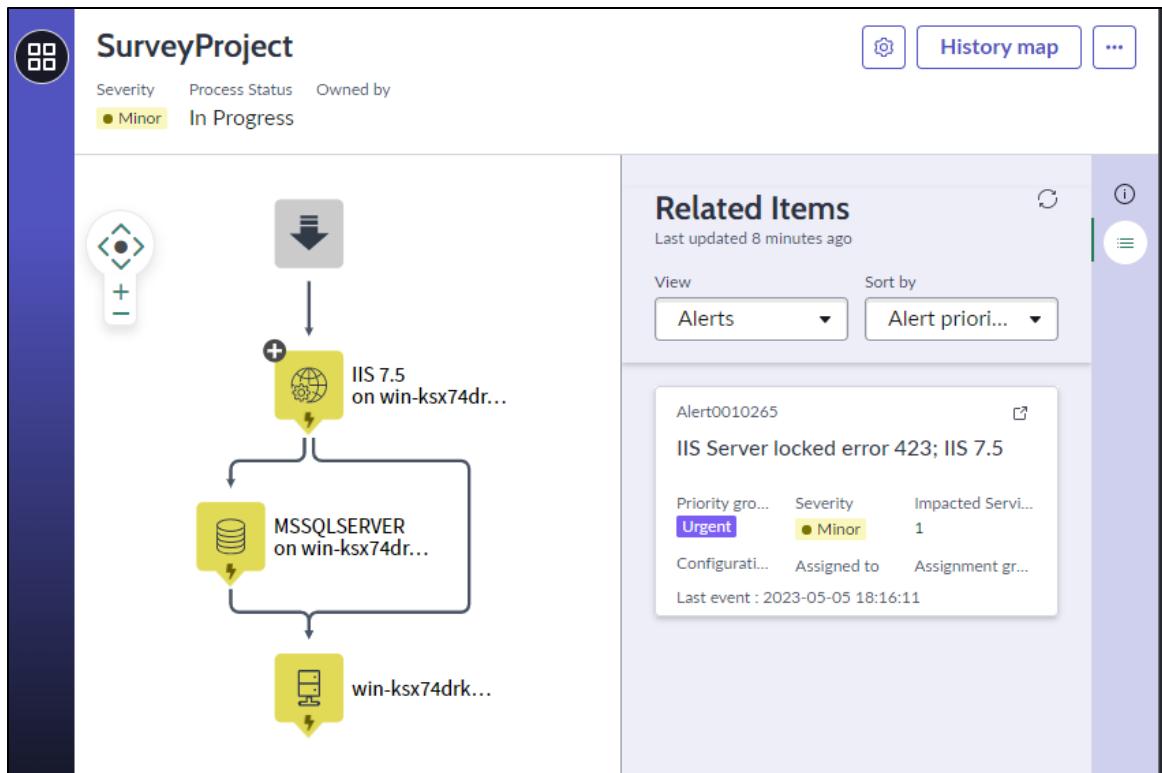
9. Open the alert created by the event.

Node	Type	Resource	Metric Name	Message key	State	Severity	Alert
Search	Search	Search	Search	Search	Search	Search	Search
win-ksx74drkgh	SNDemo	hosted application		3-3EX2017-SN1	Processed	Minor	Alert0010029

10. Note the Configuration Item matched is the server CI.

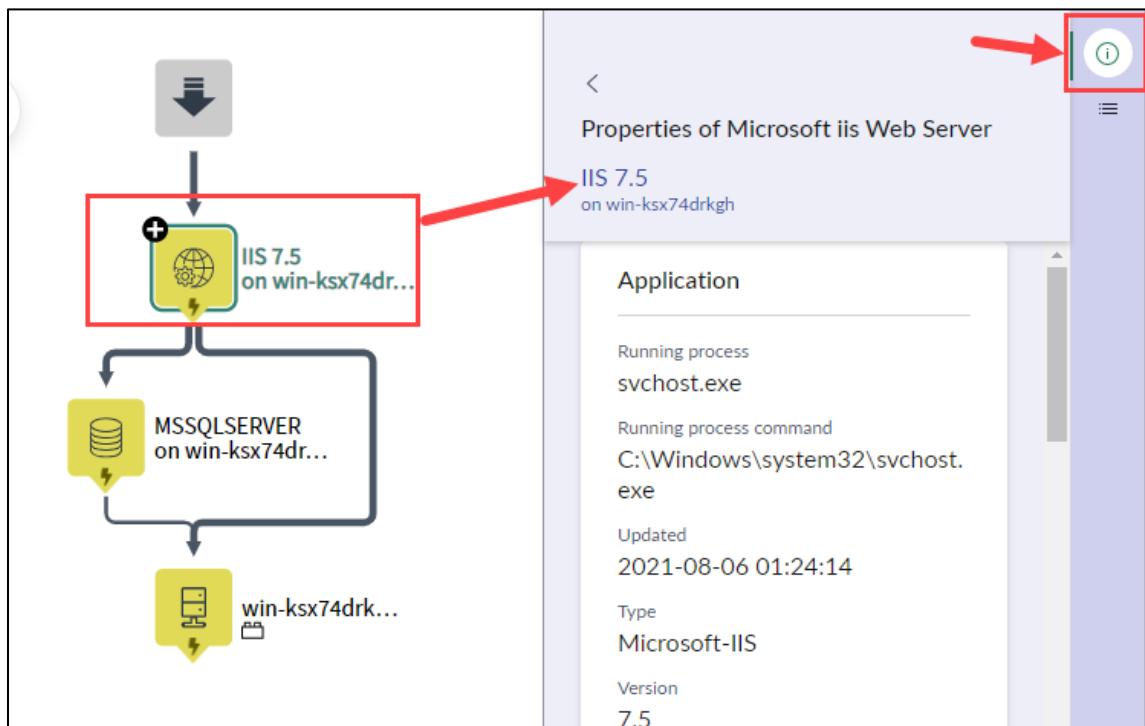
Type	SNDemo
Resource	hosted application
Configuration item	win-ksx74drkgh
Task	<input type="button" value=""/>

11. Open the **Survey Project** service map.



Note: The alert binds to the host (`win-ksx74drkgh` Windows server), impacting all CIs in the service, but the event concerns only the application (IIS 7.5 Web Server).

12. Click the **IIS 7.5 web server CI** then the **Properties icon** to see its properties.



Note: The properties pane shows the CI class attributes. Choose attributes to uniquely identify this specific CI. If the Name attribute is unique for this CI class, use it for matching.

B. Create an Event Rule with CI Field Matching

1. Navigate to Event Management > Rules > Event Rules.
2. Click the recommended rules link.
3. Expand Event group: PSScript: IIS Server locked error 423.
4. Click IIS Server locked error 423; IIS 7.5.



5. Name the Event Rule: **IIS Server Lock – Lab 3.4**.

A screenshot of the "Event Rule Info" configuration page. The page has two main sections: "Event Rule Info" on the left and "Event Filter" on the right. In the "Event Rule Info" section, there are four fields:

- Name: IIS Server Lock - Lab 3.4
- Source: PSScript
- Order: 100
- Description: (empty)

At the bottom of the "Event Rule Info" section is a checkbox labeled "Apply additional matching rules" which is currently unchecked.

6. Click **Event Filter**.

7. Populate the filter condition as follows:

All of these conditions must be met

Description	contains	IIS Server locked
Type	is	SNDemo
Resource	is	hosted application
Source instance	is	PS
Classification	is	IT
version	is	7.5

AND

8. Click **Transform and Compose Alert Output**.
9. From the **Description** field, parse out the CI name (IIS 7.5) into a variable called **name**. Delete any auto-generated expression.

Edit Regex Expressions

Original field is: **Description**
Mark or edit string to turn it into a regex expression under Transform Data

Mark Expressions	Expressions
IIS Server locked error 423; IIS 7.5	name X

Note: Because this is a new field (name), this is an example of transform.

10. The new variable is automatically added to Additional Information. Notice that version is already supplied by the event.

Classification	`\${classification}`
Additional information	`\${version}` `\${name}`

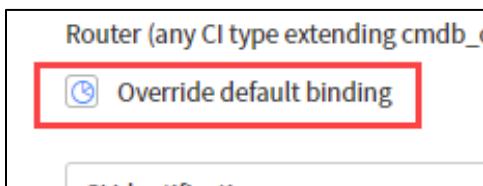
11. Blank out the Node field.

A screenshot of a software interface showing a configuration screen. A specific field labeled 'Node' is highlighted with a thick red border. Below the field are two buttons: 'Tune' and 'Cancel'.

12. From the top, click **Binding**.



13. Check the **Override default binding** option.



14. Select Binding type of **CI field matching** and CI type of **Microsoft iis Web Server**.

A screenshot of a configuration dialog for binding settings. It includes the following fields:

- Select to bind alert to CI using CI identifiers.
- Default binding: Value of Node field will be used to try and match CI name, FQDN, IP or MAC Address for Host CIs, such as Computer, OS, Switch Router (any CI type extending cmdb_ci_hw...
- Override default binding
- Binding type: CI field matching
- CI type: Microsoft iis Web Server

15. Click **Submit**.

Note: When an event matches this event rule, binding to a CI will occur only with CIs in the Microsoft IIS Web Server class, and only if the variables in Additional Information match. By clearing the Node field, alerts WILL NOT bind to the host (server) CI if a match to the web server CI fails.

C. Delete the Previously Generated Alert

1. Navigate to Event Management > All Alerts.
2. Open the **IIS Server locked error 423; IIS 7.5** alert.

3. Change the State of the alert to **Closed**.

A screenshot of a dropdown menu with the word 'State' followed by a dropdown arrow. The option 'Closed' is highlighted.

4. From **Additional actions**, select **Save**.

5. Click **Delete**.



6. Click **Delete** on the confirmation pop up window.

D. Trigger the IIS Error Event to Validate the Event Rule Binds Correctly

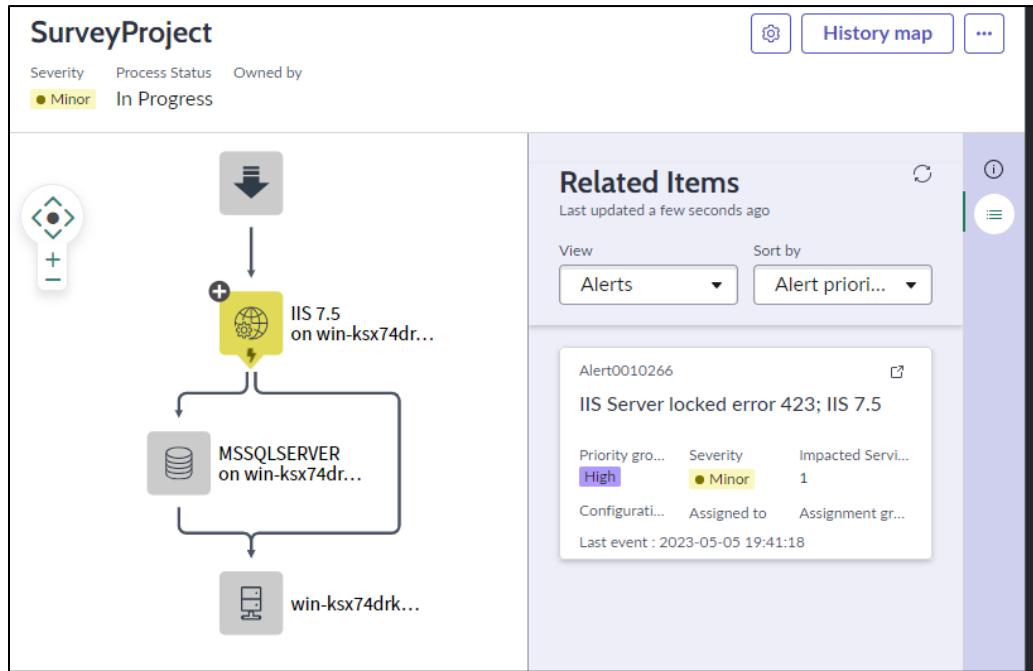
1. From the Event Generator, trigger the **Lab3.4 UnboundEvent-IIS** event once more.
2. Locate the event.

Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key
Search	Search	Search	Search	Search	Search	Search	Search
2022-02-04 15:43:30	PSScript	IIS Server locked error 423; IIS 7.5	win-ksx74drkgh	SNDemo	hosted application		3-3EX2017-SN1

3. Once the event is processed, open the event and review the Processing Notes.

Processing Notes	Binding alert CI process flow: Event CI type is cmdb_ci_microsoft_iis_web_server Query with fields: name : IIS 7.5 version : 7.5 Found one matching CI. Bounding will be done with CI id: d6fbca25b17930107f442bd6e287d024 Bind to d6fbca25b17930107f442bd6e287d024 Event rule applied: IIS Server Lock Lab 3.4
------------------	--

4. Open the **Survey Project** service map.



Note: The alert binds to the application Microsoft IIS Web Server CI (IIS 7.5), not the host Windows server CI (win-ksx74drkgh) because the event matches the new event rule.

- Open the alert on the **Survey Project** and review the configuration item bound.

This screenshot shows the details of the alert 'IIS Server locked error 423; IIS 7.5'. The 'Overview' tab is selected. In the 'Impact' section, there is a 'Configuration item' table with two rows: 'Name' (IIS 7.5) and 'Class' (Microsoft iis Web Server). A red arrow points from the text 'Close the alert.' below to the 'Name' field in this table.

Name	Class
IIS 7.5	Microsoft iis Web Server

- Close the alert.

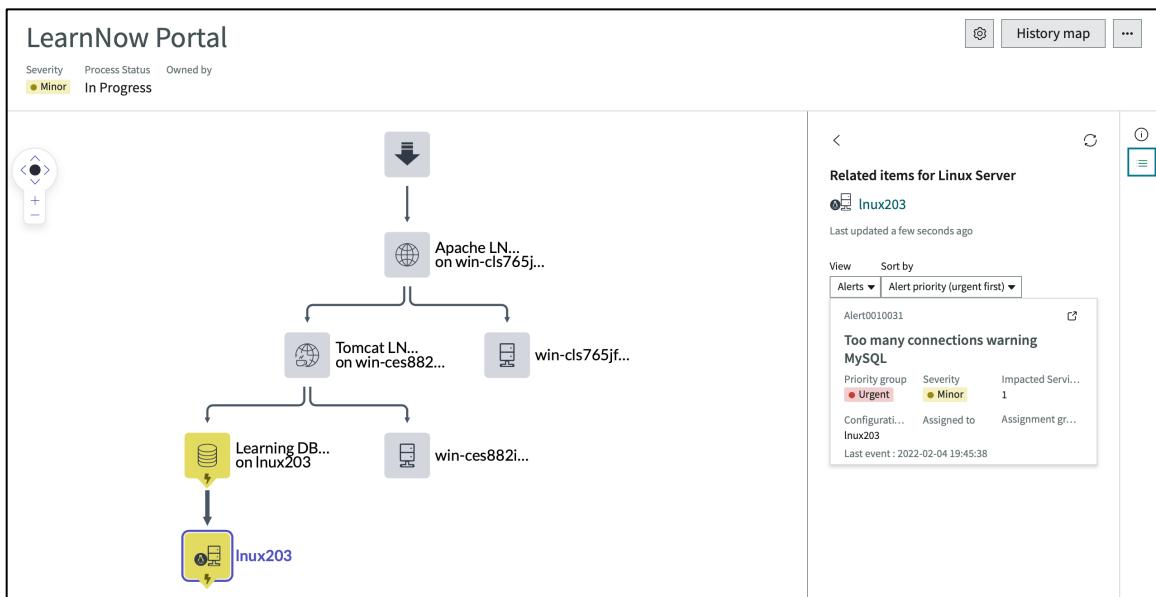
- Validate that the Survey Project displays OK .

Challenge Task: Use CI Identification Criterion Attributes to Match an Unbound Event - MySQL

- From the Event Generator, fire the **Lab3.4 UnboundEvent-mySQL**:

```
Source:          PSScript
message_key:    3-3EX2017-SN2
node:           Inux203
severity:       Minor (3)
description:    Too many connections warning MySQL
type:           SNDemo
source instance: PS
additional_info:
{'data_dir':'C:\programs\mysql\data','install_dir':'C:\programs\mysql'}
```

- Open the **LearnNow Portal** service map:



Note: The alert binds to the host CI (Inux203) but the error only affects the MySQL Instance CI (Learning DB server).

- Create an event rule with Name **MySQL connections error - Lab 3.4**.
- Using these CI identification criterion attributes for the MySQL instance CI class, configure the event rule to match the unbound event fired earlier and bind the alert to the Learning DB server, **not** Inux203.
 - sys_class_name**
 - data_directory**

- **install_directory**

IMPORTANT NOTE: Before testing the event again with your event rule, ensure you have deleted any prior alert generated from this same event.

Challenge Task: Possible Solution

All of these conditions must be met

Description	contains	connections warning MySQL
Type	is	SNDemo
Source instance	is	PS
Classification	is	IT

AND

Note: Do not blank out the node field.

Binding

Select to bind alert to CI using CI identifiers.

Default binding: Value of Node field will be used to try and match CI name, FQDN, IP or MAC Address for Router (any CI type extending cmdb_ci_hardware)

Override default binding

Binding type: CI Identification ▾

Class: MySQL Instance

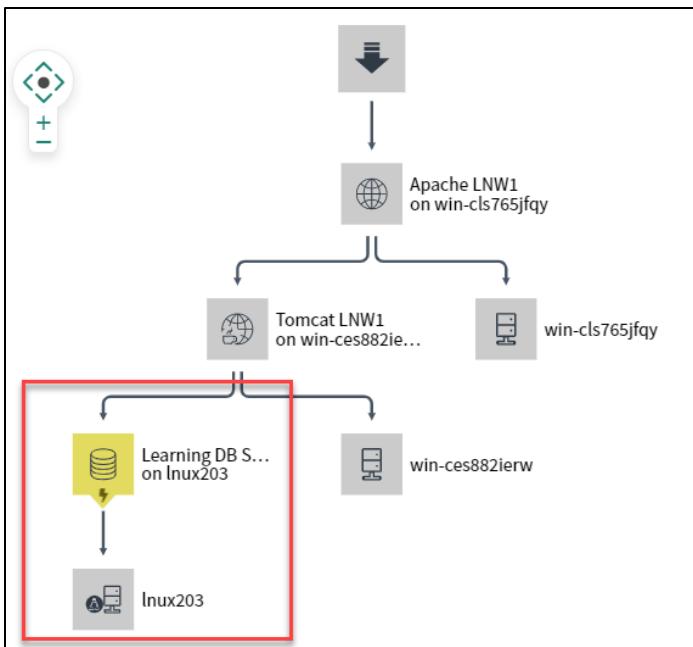
Criterion attributes - Fill at least one set of criterion attributes

data_directory	is	data_dir
install_directory	is	install_dir
sys_class_name	is	cmdb_ci_db_mysql_instance

Container level 1: Hardware

Criterion attributes - Fill at least one set of criterion attributes

name	is	Node
------	----	------



Note: The alert binds to the Learning DB server and it also impacts Tomcat LNW1 and Apache LNW1. This alert should not affect either of those CIs.

5. Close all alerts on the LearnNow Portal.

Severity breakdown	
Critical (0%)	0 Critical (0%)
Major (0%)	0 Major (0%)
Minor (0%)	0 Minor (0%)
Warning (0%)	0 Warning (0%)
OK (100.0%)	4 OK (100.0%)

Group by Business criticality ▾ Group order Ascending ▾ Segment each group by Severity ▾

Home Search services

1 - most critical (2) 2 - somewhat critical (1) 3 - less critical (1)

- Americas Calendar Portal**
- Databases**
- LearnNow Portal**
- SurveyProject**

Congratulations on completing the lab!

Event Management

Event Field Mapping Rules

Lab
3.5
20m

Lab Objectives

You will achieve the following objective:

- Use event field mapping to map nonstandard values to ServiceNow standards.

Scenario

In this lab, you fire an event with severity values that are not the ServiceNow standard. Using event field mapping, vendor severity values are mapped to appropriate ServiceNow values.

A. Execute an Infrastructure Event with a Custom Event Value

1. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**. In the upper right, click **Load Sample**.
2. In the Choose Event Sample dialog box, enter **Lab3.5** and wait for the filtered list.
3. From the list, select **Lab3.5 CustomSeverity1** and click **OK**. Notice the Additional information field containing a name:value pair representing the vendor severity.

source: Acme
message key: 3-4EX2017-SN1
description: Custom Error from ACME Monitoring
type: Acme Demo
event class: PS
additional info: acme_severity:blue

4. Click **Generate Event**.
5. You are redirected to All Events. **Refresh** the list until the event is processed.
6. Locate and **open** the event.

Time of event	Source	Description	Node	Type	Resource	Metric Name	Message key	State
Search	Search	Search	Search	Search	Search	Search	Search	Search
2022-02-04 22:08:29	Acme	Custom Error from ACME Monitoring		AcmeDemo			3-4EX2017-SN1	Error

Note: The state of the event is Error. The event has no severity value to generate an alert. The event severity in **Additional information** is **blue**. This is not a standard severity value. Due to timing, the state may temporarily read as Ready; refresh to update the state.

7. Navigate to Event Management > Rules > Event Field Mapping.

8. Create a new Event Field Mapping as shown:

- Name: **Acme Severity Lab**
- Source: **Acme**
- Mapping type: **Map field and transform value (Single field)**
- Source field: **acme_severity**
- Target field: **severity**

* Name	Acme Severity Lab	Active <input checked="" type="checkbox"/>
Source	Acme	Run after binding <input type="checkbox"/>
* Order	100	
* Mapping type	Map field and transform value (Single field)	
Filter	Add Filter Condition	Add "OR" Clause
-- choose field -- <input type="button" value="▼"/> -- oper -- <input type="button" value="-- value --"/>		
* Source field	acme_severity	* Target field severity

9. Complete the **Event Mapping Pairs** section of the record as shown (use the tab key to move through the pairs).

Event Mapping Pairs		
	Key	Value
X	green	0
X	red	1
X	orange	2
X	yellow	3
X	blue	4

Note: The baseline ServiceNow severity values are: Critical = 1, Major = 2, Minor = 3, Warning = 4, OK = 5, and Clear = 0.

10. Click **Submit**.

11. Fire the **Lab3.5 CustomSeverity1** event again.

12. Locate the new event.

Time of event ▾	Source	Description	Node	Type	Resource	Metric Name	Message key	State	Severity	Alert
Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search
2022-02-04 22:17:34	Acme	Custom Error from ACME Monitoring		AcmeDemo			3-4EX2017-SN1	Processed	Search	Alert0010032

Note: This time the event processed and generated an alert. Due to timing, the State may temporarily read as Ready; refresh to update the State.

13. Navigate to **Event Management > All Alerts**.

14. Observe the Severity of the new alert:

Number	Group	Severity	Created	Priority group	Priority	State	Source ▾	Description
Search	Search	Search	Search	Search	Search	Search	Search	Search
Alert0010032		Warning	2022-02-04 22:17:42	Low	100	Open	Acme	Custom Error from ACME Monitoring

15. Fire the **Lab3.5 CustomSeverity2** event containing “orange” severity:

source: **Acme**
 message_key: **3-4EX2016-SN2**
 description: **Custom Error from ACME Monitoring**
 type: **AcmeDemo**
 source instance: **PS**
 additional_info: **acme_severity:orange**

16. Refresh the alerts list.

Number	Group	Severity	Created	Priority group	Priority	State	Source ▾	Description
Search	Search	Search	Search	Search	Search	Search	Search	Search
Alert0010033		Major	2022-02-04 22:24:18	High	300	Open	Acme	Custom Error from ACME Monitoring

Challenge Task: Process Custom Error

1. Fire the **Lab3.5 CustomSeverity3** event:

source: **Acme**
 message key: **3-4EX2016-SN3**

description: **Process Error Level Red**
type: **AcmeDemo**
source instance: **PS**

The initial event State is Error because there is no severity specified in the event data. The severity is cited in the description text of the event. Use an event rule and regex parsing to map the severity level to the appropriate variable (acme_severity) based on the previous event field mapping and generate the alert at the correct Severity and State.

Possible Solution

For example, navigate to All Events, open the event record, click **Create Event Rule**.

Event Rule Info

Event Rule Info	
* Name	Acme Severity Challenge
Source	Acme
* Order	100
Description	

Event Filter

All of these conditions must be met

AND		All of these conditions must be met			
		Description	contains	Process Error Level	OR AND
		Type	is	AcmeDemo	OR AND
		Source instance	is	PS	OR AND
		Classification	is	IT	OR AND

Edit Regex Expressions

Original field is: **Description**

Mark or edit string to turn it into a regex expression under Transform Data

Mark Expressions

Process Error Level Red

acme_severity|

Hint: Type in "acme_severity" and hit Enter (it does not appear in the list)

Original field is: **Description**

Mark or edit string to turn it into a regex expression under Transform Data



Mark Expressions

Process Error Level Red

Expressions

acme_severity X

Number	Group	Severity	Created	Priority group	Priority	State	Source	Description
Search	Search	Search	Search	Search	Search	Search	Search	Search

Alert0010034 Critical 2022-02-04 22:52:43 High 400 Open Acme Process Error Level Red

Acknowledge the alert by opening it and clicking **Acknowledge**.



Congratulations on completing the lab!

Alerts and Tasks

Navigate Service Operations Workspace

Lab

4.1

20m

Lab Objectives

You will achieve the following objective:

- Become familiar with the operator's experience navigating Service Operations Workspace.
- Use express list to resolve alerts
- Enable the Now Assist for ITOM skill (alert analysis)
- Review alert content in SOW.

Scenario

In this lab, navigate Service Operations Workspace to see how operators work to resolve alerts and tasks through the express list. Now Assist for ITOM is installed, but the skill is not activated. You will activate the skill then test alert analysis.

A. Explore an Alert in Service Operations Workspace

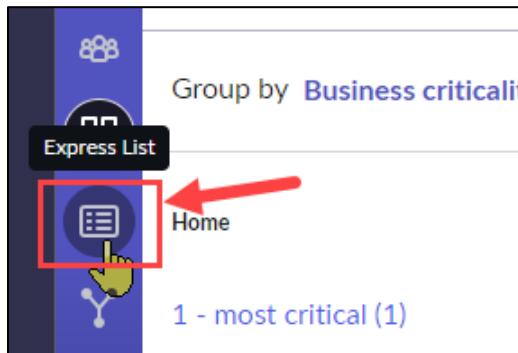
This section introduces managing alerts in Service Operations Workspace reusing a sample event from an earlier lab.

1. Navigate to **Event Management > Simulation > Event Generator**.
2. Click **Load Sample**.
3. Select **Lab2.3 VMerror1** and click **OK**.

source:	PSScript
node:	{your MID private IP address entered in lab 2}
severity:	Critical (1)
description:	Critical service error (print spooler)
type:	SNDemo
source instance:	PS
additional_info:	{"remediation_action_resource":"Print Spooler"}

4. Click **Generate Event**.

5. You are redirected to All Events. **Refresh** the list until the event is processed.
6. Navigate to **Service Operations Workspace** express list.

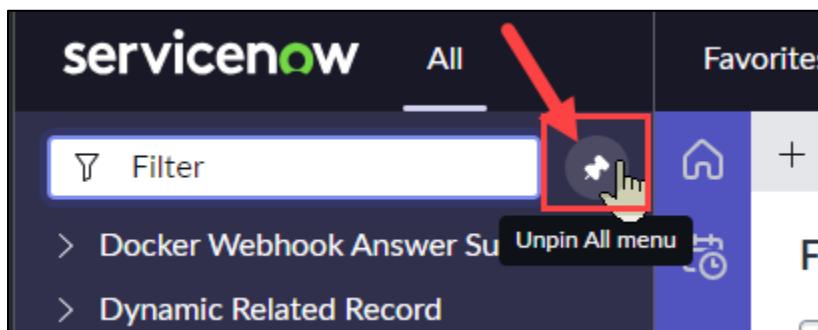


7. The Active alerts (Default) list is opened.

A screenshot of the Active alerts (Default) list. The sidebar on the left shows various filters like State, updated, Severity, Priority group, and Source. The main area displays a table of four alerts:

Number	Description	Duration	Severity
Alert0010040	Critical service error (print spooler)	6 minutes	Critical
Alert0010038	Custom Error from ACME Monitoring	17 hours	Major
Alert0010037	Custom Error from ACME Monitoring	17 hours	Warning
Alert0010004	This is a Test for Lab 1.1	2 days	Minor

8. If you have the application navigator pinned, un-pin it.



9. With the application navigator closed, express list options on the top right are visible.

severity Priority Source Impacted service

Critical High PSScript

Note: Hiding the express list filter panel also exposes these buttons.

10. The list is sorted by Duration by default. Click on column headers to sort by that column.

Number	Description	Duration	Severity	Priority	Source	Impacted service
Alert0010040	Critical service error (print spooler)	20 minutes	Critical	High	PSScript	
Alert0010038	Custom Error from ACME Monitoring	17 hours	Major	Moderate	Acme	
Alert0010037	Custom Error from ACME Monitoring	17 hours	Warning	Low	Acme	

11. Use the Time range picker in the upper right to limit the number of alerts shown.

Time range picker

severity Priority Source

Warning Urgent Se

Warning Low Ac

Major Moderate Ac

Critical High PS

Last 15 min
Last hour
Last 12 hours
Last 24 hours
Last 2 days
Last week
All time
Custom

12. Click in the row for the latest alert (Critical service error) which will open the side panel.

The screenshot shows the 'Active alerts' list on the left and a detailed view of a specific alert on the right. The alert details are as follows:

- Critical service error (print spooler)**
- Duration:** 2 hours
- Configuration item:** ip-198-51-191-37
- Metric name:** 198.51.191.37
- Source:** PSScript
- Last updated:** 2024-05-10 16:48:29

Note: *that in the side panel, there is no Now Assist feature.*

13. Hover over the left center edge of the side panel to expose the handles which allow resizing of the panel.

A screenshot of the alert details page. A red double-headed arrow points to the vertical resize handle located on the left edge of the panel. A cursor is hovering over this handle.

14. Open the latest alert (Critical service error (print spooler)) by clicking the alert number.

A screenshot of the 'Active alerts' list. A mouse cursor is hovering over the 'Number' column of the first alert, which is 'Alert0010040'. The alert details are partially visible on the right.

15. The alert is composed of several tabs. Note that on the Overview tab there is no Now Assist feature.

The screenshot shows the ServiceNow interface for an alert titled "Critical service error (print spooler)". The top navigation bar includes "Express List" and the alert ID "Alert0010040". Below the title, it displays priority group (High), severity (Critical), state (Open), and initial event generation time (2024-05-10 16:48...). A vertical sidebar on the left contains icons for Home, Express List, Critical, Details, Related records, Metrics, and Playbook. The main content area has tabs for Overview, Details, Related records, Metrics, and Playbook, with "Overview" highlighted. A red box highlights the tabs. Below the tabs is a "Summary" section. Under "Identified issue", the description is "Critical service error (print spooler)".

16. Note the Utilities pane on the right. Also note the bound CI is a Windows Server.

The screenshot shows the same alert page as above, but with a larger Utilities pane on the right. The Utilities pane contains two sections: "Launch App" (Search Google) and "Dependency View". In the main content area, the "Configuration item" section is expanded, showing a table with one row: Name (ip-198-51-187-43) and Class (Windows Server). A red box highlights this table.

17. Review the information by scrolling down in each tab.

18. Click on the **Playbook** tab and note the only remediation action on this alert with a Windows server CI is Create Incident. This is due to an active alert management rule. In a later lab you will add additional baseline Windows Server remediation actions.

19. Click the **Agent Assist** button on the right.

Note: The **Knowledge Articles** section provides a list of suggested knowledge base articles that may help you resolve the current alert (based on keywords in the short description).

20. In the **Related records** tab, click **Events**.

Overview Details Related records Metrics Playbook

Events (4) Events 4

Last refreshed just now.

Severity	Time of event ▾	Source	Node	Type
Critical	2022-07-14 20:59:59	PSScript	198.56.1.200	SND
Critical	2022-07-14 20:55:59	PSScript	198.56.1.200	SND
Clear	2022-07-14 20:53:08	PSScript	198.56.1.200	SND

Note: This displays all the events that either triggered or cleared the alert. Your events may differ.

21. Click the **Details** tab and review the **Activity** stream.

Urgent Critical Reopen 2022-07-14 20:48... INC0010004

Overview Details Related records Metrics Playbook

Alert

Number: Alert0010034

Configuration item: IIS 7.5

Metric name: Microsoft IIS Web Server

Class: Microsoft IIS Web Server

Owner by: Microsoft IIS Web Server

Maintenance Acknowledged

Assigned to:

Assignment group:

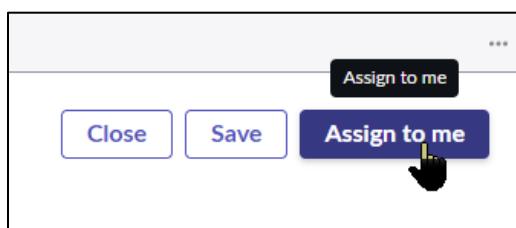
State:

Activity

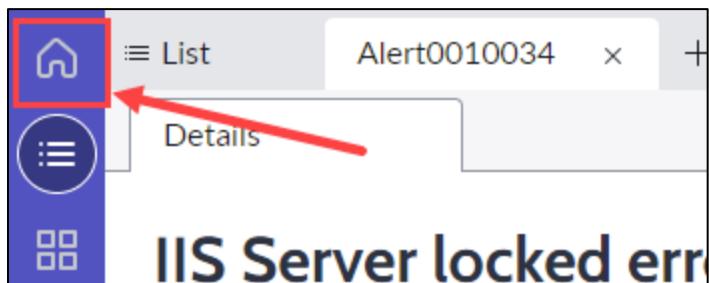
- System Work notes • 2022-07-14 21:00:20 Task is created by System Administrator, using "Windows IIS Service" Alert Rule.
- System Work notes • 2022-07-14 21:00:07 Updated alert state from Closed to Reopen due to event: IIS Server locked error 423
- System Administrator Work notes • 2022-07-14 20:58:49

Activity provides a timeline of all actions relating to this alert. It is very helpful in understanding a sequence of events. Your number of executions and incident numbers may vary.

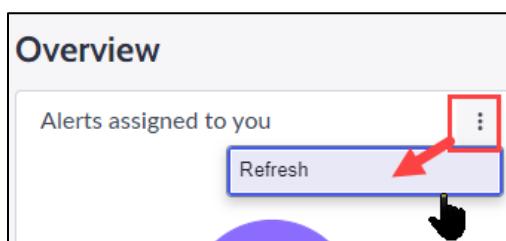
22. Click **Assign to me**.



23. Click the **Home** button



24. Refresh the Alerts assigned to you tile.



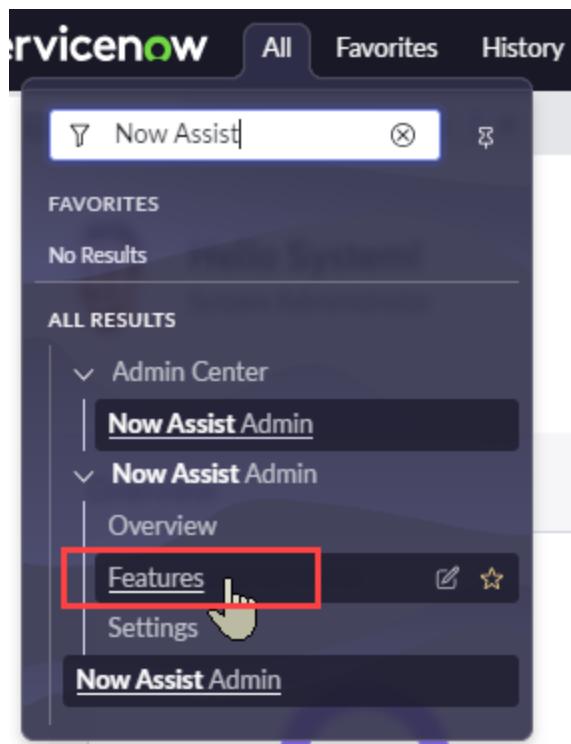
Note: Alert related tiles are enabled with the evt_mgmt_operator role, which has been granted to admin in this training environment.

25. Click **Show all records** to display alerts assigned to you.

Number	Description	Group	Priority group	Severity	State	Configuration
Alert0010034	IIS Server locked error 423	None	Urgent	Critical	Reopen	IIS 7.5

B. Enable the Now Assist alert assist skill.

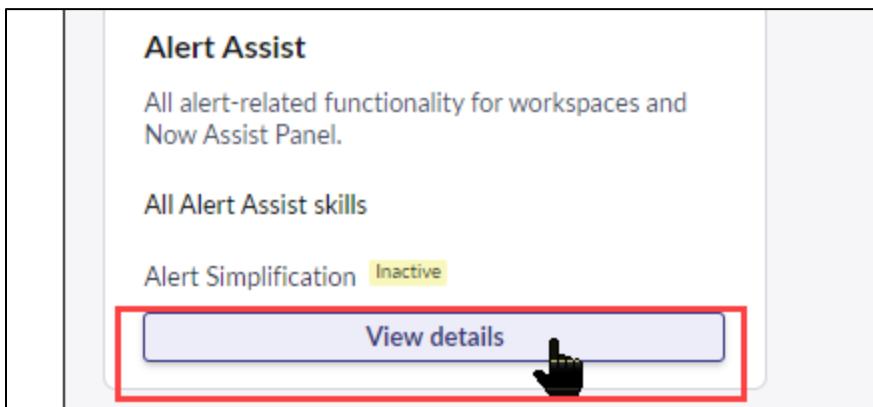
1. Navigate to Now Assist Admin > Features.



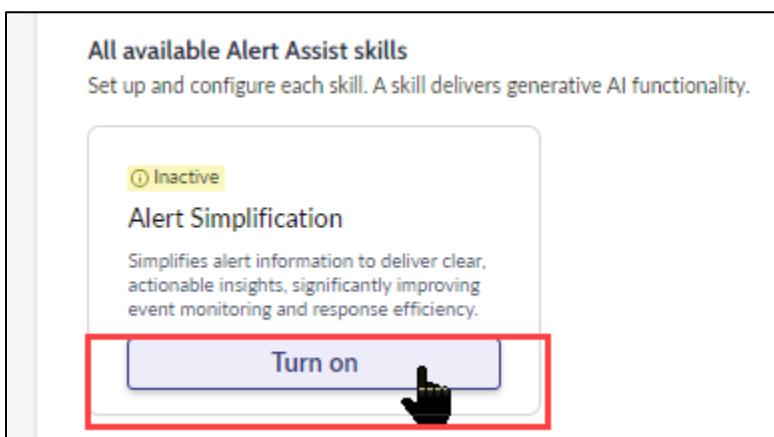
2. In the Technology flow, use the dropdown to select ITOM.

A screenshot of the "Now Assist Features" page for the "Technology" product. The top navigation bar includes "Overview", "Now Assist Features", and "Settings". The left sidebar lists "Technology", "Customer", "Employee", "Creator", and "Platform", with "Technology" highlighted by a red box. The main content area shows the title "Now Assist skills for Technology" and the sub-instruction "Explore Now Assist skills for Technology products.". Below this is a "Select product" dropdown menu with "ITSM" selected. A second dropdown menu shows "ITSM" and "ITOM", with "ITOM" highlighted by a blue box and a hand cursor pointing at it. A yellow banner at the bottom right of the main content area says "Install the ITSM plugin to explore all skills.".

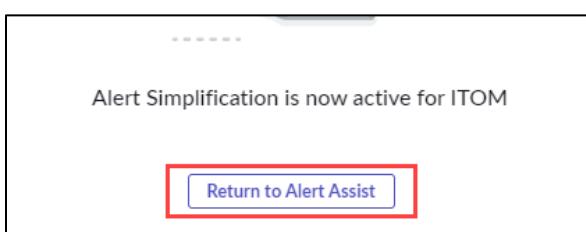
3. Click **View Details**.



4. Click Turn on.

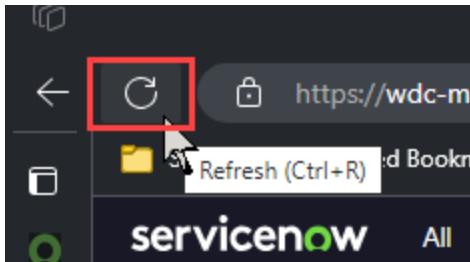


5. Close the pop-up.



6. Return to Service Operations Workspace **express list**.

7. Refresh the browser tab.



8. Wait a few seconds for the list. If necessary, use the time range picker.

Number	Description	Duration	Severity	Priority	Source
Alert0010040	Critical service error (print spooler)	2 days	Critical	High	PSScript
Alert0010038	Custom Error from ACME Monitoring	3 days	Major	Moderate	Acme
Alert0010037	Custom Error from ACME Monitoring	3 days	Warning	Low	Acme
Alert0010012	There are 3 alerts which were not updated f...	3 days	Minor	Urgent	
Alert0010004	This is a Test for Lab 1.1	5 days	Minor	Low	PSScript

9. Click the row for your most recent alert (Critical service error).

10. The Now Assist skill now appears in the side panel.

Alert0010040 Open
Critical service error (print spooler)

(ip_address: 198.51.191.37) (location:)

Info Probable cause (0)

Alert summary by Now Assist Summarize

Duration 3 hours
2024-05-10 16:48:29 (Initial event generation time)

Configuration item ip-198-51-191-37

Incidents on configuration item (0)
Incidents on related configuration items (0)

Metric name

11. Open the alert by clicking the **alert number**. The Now Assist function appears on the Overview tab. Click **Summarize**.

Critical service error (print spooler) ⓘ

Priority group: High Severity: Critical State: Open Initial event generation time: 2024-05-10 16:48...

Overview Details Related records Metrics Playbook

+ Alert summary by Now Assist

Summary

Summarize

12. Wait a few seconds for the analysis to complete.

Alert summarized by Now Assist ⓘ

Summary:

- Critical service error (print spooler)
- A critical service error has occurred in the print spooler. This could cause printing issues and should be addressed immediately.

Alert analysis:

The print spooler is a critical component of the printing process. If this error is not resolved quickly, it could cause printing issues and affect the entire organization's ability to print documents. The recommended course of action is to investigate the issue immediately and take steps to resolve it.

Be sure to check AI-generated summaries for accuracy.

13. Close the alert.



Congratulations on completing the lab!

Alerts and Tasks

Alert Management Rules

Lab
4.2
20m

Lab Objectives

You will achieve the following objectives:

- Create an alert management rule to generate an incident
- Observe automatic incident generation
- Handle an incident
- Activate a baseline alert management rule with remediation actions
- Modify a Flow Designer subflow

Scenario

In this lab, the shutdown of the IIS Web Service supporting the Survey Project service generates an event. The event generates an alert displaying the Survey Project service in a critical state which then triggers an incident to address the failed web service. Resolving the incident closes the alert.

In the second half of the lab, you will activate a baseline alert management rule whose filter matches Windows Server class CIs and makes remediation actions available from the alert. To better understand Flow Designer, you will modify and republish a baseline subflow that restarts a Windows service through remote PowerShell commands.

ServiceNow Now Learning has a suite of Flow Designer courses in the learning path *Flow Designer Essentials*.

A. Confirm Incident Control Properties

1. Navigate to **Event Management > Administration > Event Management Properties**.

2. Ensure these properties are set as shown:

The screenshot shows a configuration dialog with the following settings:

- Closing alerts will:** Resolve Incident
- Reopening alerts will:** Create New Incident
- Enable Avoid Incidents on Secondary alerts and wait for Grouping job to be executed:** No (checkbox is unchecked)
- Resolving an incident closes the associated alerts:** Yes (checkbox is checked)

3. If not set by default, click **Save**.

B. Create an Alert Management Rule to Trigger Incidents

1. Navigate to **Event Management > Rules > Alert Management Rules**.
2. Sort the rules by name and review the baseline rules. Note that *Create Incident Manually* is active, which made the *Create Incident* playbook action available in earlier labs.

The screenshot shows a table of alert management rules:

Name	Description	Active	Or
Create Incident	OOB rule. Create an incident for all ale...	false	
Create Incident for Primary Alert	OOB rule. Manually create an incident for all alerts that are not in maintenance state.	false	
Create Incident Manually	OOB rule. Manually create an incident fo...	true	
Create Incident on Primary Critical Alert	OOB rule. Create an incident for primary...	false	

Note: Baseline rules can be copied and customized, or new rules can be created.

3. Create a **New** alert management rule as shown:

- Name: **Windows IIS Service**
- Order: **50**

* Name	Windows IIS Service	* Order	50
Active	<input checked="" type="checkbox"/>	Multiple alert rules	Search for additional rules ▾

4. Select the **Alert Filter** tab and enter the following information as shown:

- Rule is activated when: **Alert matches filter**

And alert filter **CONDITIONS** of:

- **Short description** |contains| **IIS** **AND**
- **Severity** |is| **Critical**

The screenshot shows the 'Alert filter' configuration screen. The 'Rule is activated when' dropdown is set to 'Alert matches filter'. The 'Conditions' section is expanded, showing two AND clauses: 'Short description contains IIS' and 'Severity is Critical'. The entire 'Conditions' section is highlighted with a red box.

Note: Alert management rules with lower order values are given priority. An alert is checked against every alert management rule until a match is found.

5. Select the **Actions** tab.

6. In the **Remediation Subflows** section, under the **Subflow** heading, double-click on **Insert a new row....**

The screenshot shows the 'Remediation Subflows' section. A button labeled 'Insert a new row...' is highlighted with a green box and a hand cursor icon is placed over it.

7. Enter/select a **Subflow** value of **Create Incident**.

The screenshot shows the 'Remediation Subflows' search interface. A search bar at the top contains the text 'Create'. Below it, a message says 'Showing 1 through 2 of 2'. Two items are listed: 'Create Incident' and 'Create Task (legacy)'. The 'Create Incident' item is highlighted with a blue background.

- Click the green checkmark to set the value.

The screenshot shows the same search interface as above, but with a hand cursor pointing at the green checkmark icon next to the 'Create Incident' entry.

The screenshot shows the 'Remediation Subflows' list view. A single row is selected, showing the following details:

	Subflow	Execution	Automatic executions limit	Active	Link to Flow Designer
	Create Incident	Automatic	1	true	

Note: **The Execution, Automatic executions limit, and Active fields are set to default values. The Link to Flow Designer is filled in once you submit the alert management rule.**

- Click **Submit**.

- To view the updated actions, open the rule from your list of alert management rules and click on the **Actions** tab.

The screenshot shows the 'Alert Management Rules' interface. The 'Actions' tab is selected. A message box at the top says: 'Specify alert rule response to alert using pre-defined remediation subflows from ServiceNow Flow Designer. Use it to create incident, send mail, update alert, etc. Specify automatic or interactive type to control execution.' Below this is a 'Remediation Subflows' list view. A single row is highlighted with a red box, showing the following details:

	Subflow	Execution	Automatic executions limit	Active	Link to Flow Designer
	Create Incident	Automatic	1	true	/flow-designer.do?sysparm_nostack=true#/sub-flow-designer/45454f6193330300415c74aff67fffb

C. Generate an IIS Service Down Event

1. Close any necessary alerts to make Survey Project green on the Event Management Service Operations Workspace.



2. In your ServiceNow instance, navigate to **Event Management > Simulation > Event Generator**.
3. Click **Load Sample**.
4. Select **Lab4.1 IISError** and click **OK**.

```
source:          PSScript
node:           198.56.1.200
message_key:    4-1EX2017-SN1
severity:       Critical (1)
description:    IIS Server locked error 423
type:           SNDemo
source instance: PS
additional_info: {'version':'7.5'}
```

5. Click **Generate Event**.
6. You are redirected to All Events. **Refresh** the list.

7. Wait for Survey Project to show critical.



8. Navigate to **Event Management > All Alerts**.

9. Locate the alert and **open** the corresponding **incident**.

State	Source	Description	Node	Configuration item	Metric Name	Maintenance	Task	Impact
Search	Search	Search	Search	Search	Search	Search	Search	Search
402 Open	PSScript	IIS Server locked error 423	198.56.1.200	IIS 7.5		false	INC0010002	
306 Closed	PSScript	Network Interface Error on	198.56.1.203	win-cls526aazp		false	(empty)	

Note: An alert and an incident generate from the IIS Server locked error event. It may take ~45 seconds or so for the incident to display under the Task column.

Your incident number may vary.

10. Observe the key values on the incident form inherited from the event: **Configuration item**, **Urgency**, and **Short description**.

Number	INC0010002	Contact type	-- None --
* Caller	Event Management	State	New
Category	Inquiry / Help	Impact	3 - Low
Subcategory	-- None --	Urgency	1 - High
Service		Priority	3 - Moderate
Configuration item	IIS 7.5	Assignment group	
* Short description	IIS Server locked error 423	Assigned to	
Description	Critical alert [Alert0010035] . Created on Cl: [IIS 7.5] . Metric name is [] of type [SNDemo] from data source [PSScript]. Total impacted services by the Cl: [IIS 7.5] is 1.		

D. Resolve the Incident

1. Scroll down to select the **Resolution Information** tab, and complete the form as shown:
 - Resolution code: **Resolved by change**
 - Resolution notes: **Applied Microsoft hot fix 5.2**

The screenshot shows the 'Resolution Information' tab selected in a ServiceNow interface. The form includes fields for 'Knowledge' (checkbox), 'Resolution code' (dropdown set to 'Resolved by change'), and 'Resolution notes' (text area containing 'Applied Microsoft hot fix 5.2').

2. Click **Resolve**.



3. Return to the **All Alerts** list, locate the alert and view its current State is Closed.

All > Role in Group != Secondary > Role in Group != Both Primary and Secondary								
	Number ▲	Group	Severity	Priority group	Priority	State	Source	Description
	Alert0010028		● Critical	● Urgent	2406	Closed	PSScript	IIS Server locked error 423

Note: *The alert closed when the incident was resolved. This may take a few seconds. Refresh the list if needed.*

E. Activate a Baseline Alert Management Rule with Remediation Actions

1. Before enabling baseline rules in your production environment, check the documentation for the latest requirements (*Configure alert remediation actions*). In our training environment, you will just need to add the credential and credential

alias, as that is unique to each student environment. In this lab, the credential is the Windows Server Administrator account and the alias makes that credential available to the baseline flows.

Documentation excerpt (do not perform the following bullets):

Before you begin

Install the IntegrationHub Enterprise spokes plugin.

For Linux: Ensure that the remote Linux host is reachable using the MID Server IP address that runs action scripts.

For Windows:

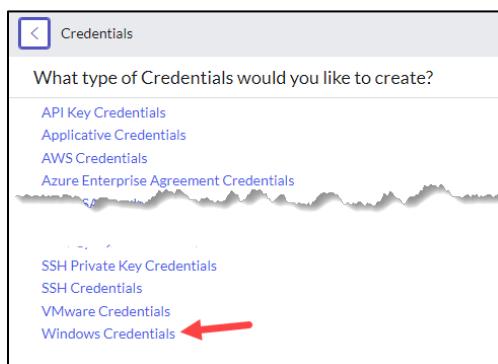
- Ensure that Powershell v3.0 - 5.0 are supported and installed on the Windows target servers.
- Enable Powershell remoting on the remote Windows host.
- Ensure that the remote Windows host is reachable using the MID Server FQDN that runs action scripts.

Add credentials to the credential aliases that come with the base system:

- linuxAdmin
- windowsAdmin

Role required: evt_mgmt_admin or flow_designer

2. Create the credential and alias: Navigate to **Service Mapping > Credentials**.
3. Click **New**.
4. Click **Windows Credentials**.



5. Fill in the form with:
 - Name = **windows_mid Admin**
 - Applies to = **All MID servers**
 - User name = **workgroup\Administrator**
 - Password = copy/past your Windows Server password from your Now Learning landing page. Ensure you do not copy any extra spaces.

Powershell is required to use Windows credentials.

Name	<input type="text" value="windows_mid Admin"/>	Applies to	<input type="text" value="All MID servers"/>
Active	<input checked="" type="checkbox"/>	Order	100
If the user is part of a domain or workgroup, prefix the user name with this value (ex. domain\user). The prefix '\' may be used to enforce the use of a local user account.			
User name	<input type="text" value="workgroup\Administrator"/>		
Password	<input type="password" value="*****"/>		
A connection alias resolves your connection and credential at runtime. More than one Credential can be active per Connection Alias at a time. If more than one credential is active, they will be used in order.			
Credential alias		Use MID Server Service Account	<input type="checkbox"/>

6. Click the icon to unlock credential alias.

A connection alias resolves your connection and credential at runtime. More than one credential can be active per Connection Alias at a time. If more than one credential is active, they will be used in order.

Credential alias	
Use MID Server Service Account	<input type="checkbox"/>

Note: *Credential alias field appears on the Default view of the Windows Credentials form.*

7. Search for *windows and select sn_em_connector.windowsAdmin.

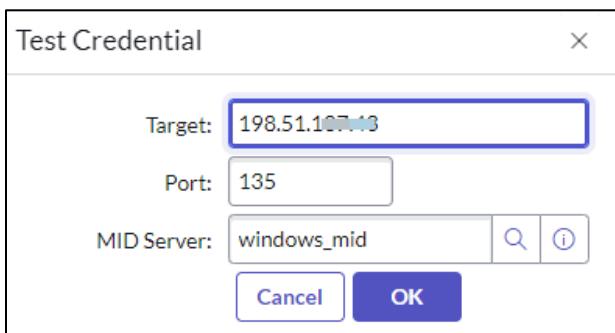
Credential alias	
Use MID Server Service Account	<input type="text" value="*windows"/> sn_acc_spoke.Agent_Client_Collector_Windows
	 sn_em_connector.windowsAdmin

8. Click the icon to **Lock Credential alias**.

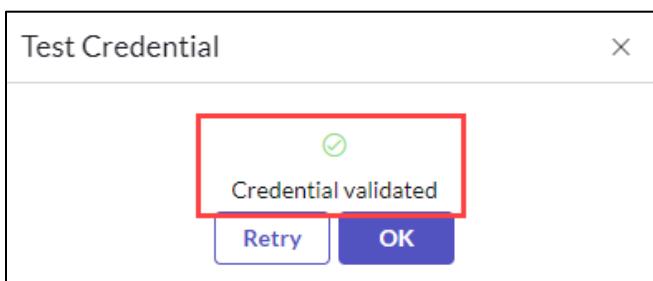


9. In Related Links, click **Test credential**.

10. In the pop-up window, enter your Windows MID Server **private IP address**.



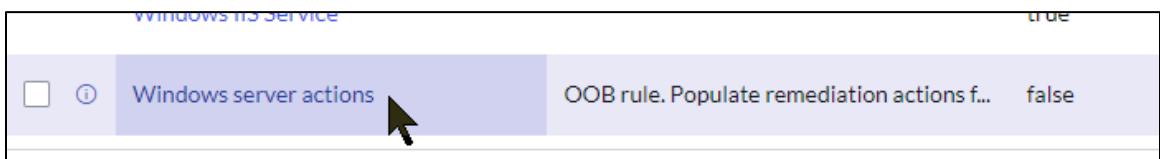
11. Click **OK**. **ENSURE THE CREDENTIAL WORKS** (is validated). If it fails, return to the credential record, delete and re-add the password. Ensure you do not copy/paste any extra space characters. The credential must work before proceeding. If necessary, carefully type it in.



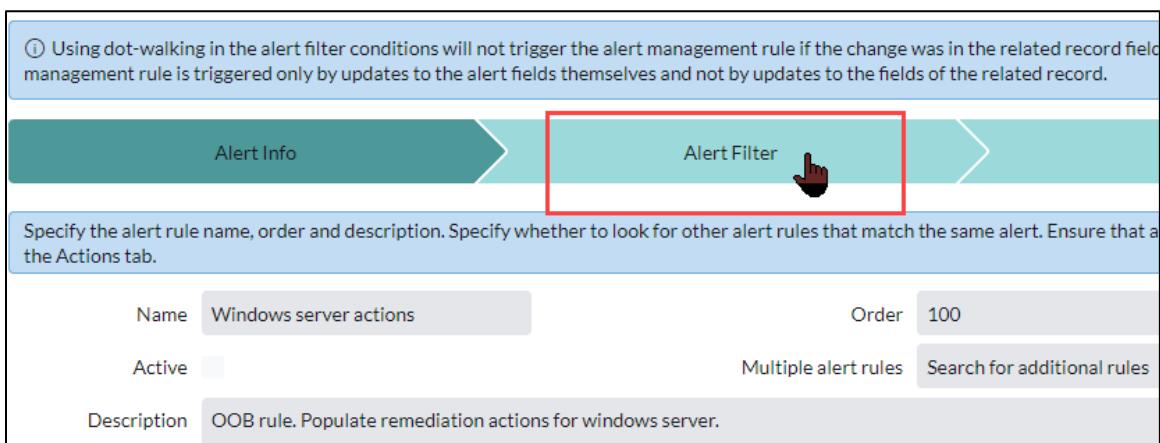
12. Once your credential tests successfully, click **Submit**. Your credential alias is ready to be used by the baseline remediation subflows.

13. Navigate to **Event Management > Rules > Alert Management Rules**.

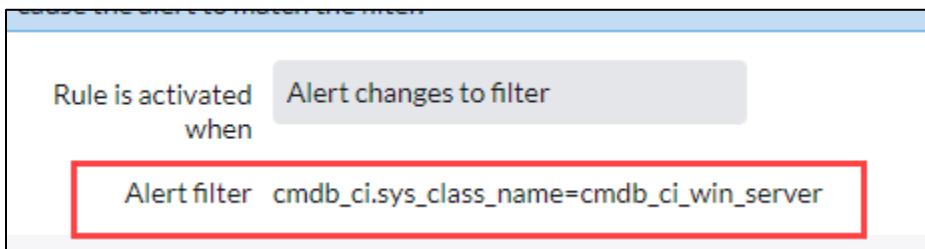
14. Locate and open the **Windows server actions** rule.



15. Review the Alert Info tab and click **Alert Filter**.



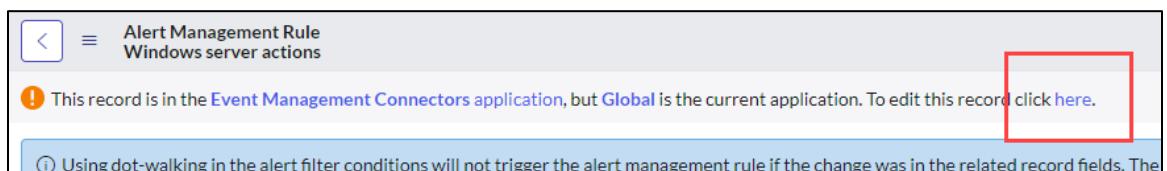
Note: *The filter applies the rule to all windows server CIs.*



16. Click **Actions**. Review the list of included baseline Flow Designer subflows made available to alerts matching the filter.

Subflow	Execution	Automatic executions limit	Active	Link to Flow Designer
Get Windows Processes	Manual	1	true	/\$flow-designer.do?sysp
Start Windows Service	Manual	1	true	/\$flow-designer.do?sysp
Stop Windows Service	Manual	1	true	/\$flow-designer.do?sysp
Suspend Windows Service	Manual	1	true	/\$flow-designer.do?sysp
Stop Windows Process	Manual	1	true	/\$flow-designer.do?sysp
Get Windows Services	Manual	1	true	/\$flow-designer.do?sysp
Restart Windows Service	Manual	1	true	/\$flow-designer.do?sysp

17. In the notification line, click to edit the record.



18. On the Alert Info tab, select **Active**.

The screenshot shows the 'Alert Info' tab for the 'Windows server actions' rule. It has tabs for 'Alert Info' and 'Alert Filter'. The 'Alert Info' tab contains fields for 'Name' (set to 'Windows server actions'), 'Active' (with a checked checkbox), and 'Description' (set to 'OOB rule. Populate remediation actions for windows server.'). A red arrow points to the 'Active' checkbox.

19. Click **Update** to activate the rule.



20. Navigate to **Event Management > Simulation > Event Generator**.

21. Click **Load Sample**.

22. Select **Lab2.3 VMerror1** and click **OK**.

```

source:      PSScript
node:       {your MID private IP address entered in lab 2}
severity:   Critical (1)
description: Critical service error (print spooler)
type:        SNDemo
source instance: PS
additional_info: {"remediation_action_resource":"Print Spooler"}

```

23. Click **Generate Event**.

24. You are redirected to All Events. **Refresh** the list until the event is processed.

25. Click to **open** the alert. Make a note of the alert number as you will come back to it later.

Message key	State	Severity	Alert
-2.1WIN2017	Processed	Critical	Alert0010014

26. In the menu bar or Related Links, click **Quick Response**. Note the remediation actions made available by the alert rules. It may take a minute for the form to render.

Quick Response for Alert0010074 X

Click the appropriate link either to run remediation or to launch a web application

Run Remediation Create Incident Get Windows Processes Get Windows Services Restart Windows Service Start Windows Service Stop Windows Process Stop Windows Service Suspend Windows Service	Launch Application Dependency View Search Google
---	---

27. Click **X** to close the popup.

28. Click **Open in Workspace**.

29. Review the alert in Service Operations Workspace. Note the CI class is Windows Server.

The screenshot shows the 'Overview' tab selected in the top navigation bar. Below it, the 'Summary' section contains an 'Identified issue' box with a description: 'Critical service error (print spooler)'. In the 'Impact' section, there is a 'Configuration item' box. Inside this box, a table shows a single row with 'Name' (jp-198-51-187-43) and 'Class' (Windows Server). The 'Name' cell is highlighted with a red border.

30. Click the **Playbook** tab. The same remediation actions appear here.

The screenshot shows the 'Playbook' tab selected in the top navigation bar. The main title is 'Critical service error (print spooler)'. Below it, the 'Priority group' is 'High', 'Severity' is 'Critical', 'State' is 'Open', and 'Initial event generation time' is '2023-01-25 22:16...'. The 'Alert remediation' section lists several actions:

- Action: Stop Windows Process
- Action: Get Windows Processes
- Action: Stop Windows Service
Last executed at 2023-01-27 19:05:44
- Action: Restart Windows Service
Last executed at 2023-01-30 20:11:13
- Action
- Action

F. Modify a Flow Designer Subflow

This section will introduce you to Flow Designer. Flow Designer is the engine for the remediation actions made available by alert management rules. The baseline remediation subflows for Windows Servers use remote PowerShell to execute commands on target servers.

Note: The Restart Windows Service subflow, as well as the other Windows remediation subflows, retrieves the fully qualified domain name from the CI record and uses it as the target computer for the PowerShell script. In our training environment, the Windows MID Server is not joined to a domain. The resulting FQDN created by Discovery is not resolvable by PowerShell. You will need to modify the subflow to use IP address instead. Here is an example of the resulting error using FQDN:

Activity

System Administrator
Work notes • 2023-01-31 00:02:03

PowerShell script execution failed. Script returned status 1 using account user workgroup\Administrator.

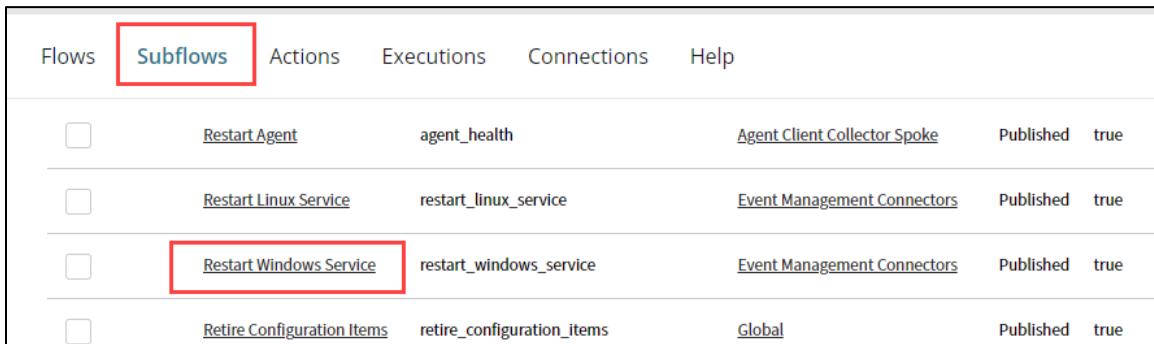
Note: The event produced from the event source should contain the Windows service in trouble. Use event rules to parse the service into the alert additional information field in the form "remediation_action_resource": "<service display name>" for the remediation action to act on that service.

Description	Critical service error (print spooler)
Additional information	{"remediation_action_resource": "Print Spooler"}

In this lab, you will edit the subflow and replace the FQDN with IP address.

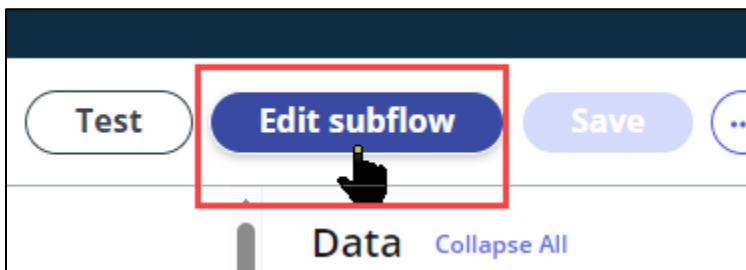
1. Navigate to **Process Automation > Flow Designer**.
2. Click **Subflows**.

3. Open the **Restart Windows Service** subflow.

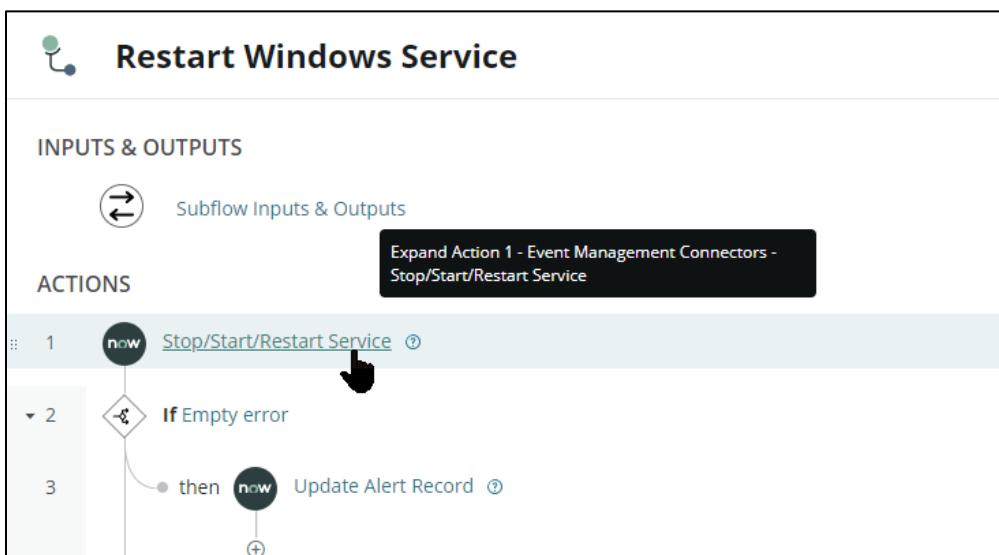


<input type="checkbox"/>	Restart Agent	agent_health	Agent Client Collector Spoke	Published	true	
<input type="checkbox"/>	Restart Linux Service	restart_linux_service	Event Management Connectors	Published	true	
<input type="checkbox"/>	Restart Windows Service	restart_windows_service	Event Management Connectors	Published	true	
<input type="checkbox"/>	Retire Configuration Items	retire_configuration_items	Global	Published	true	

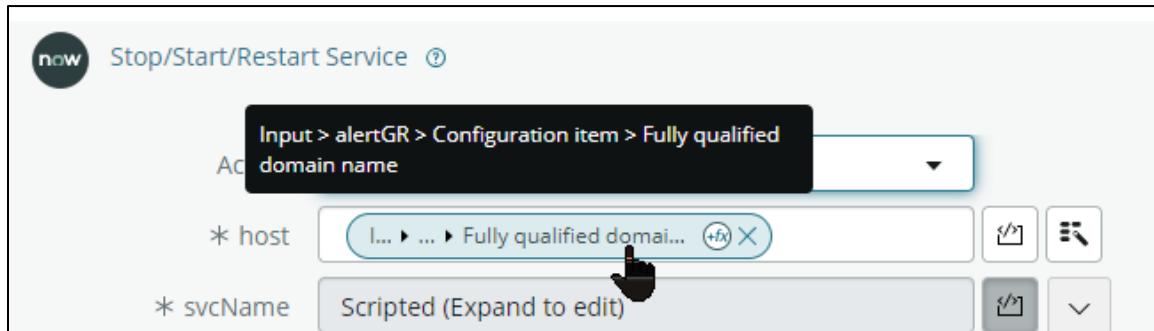
4. In the upper right, click **Edit subflow**.



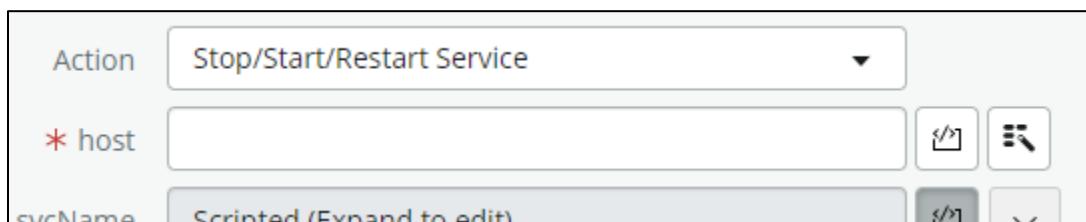
5. In Actions, expand **Stop/Start/Restart Service**.



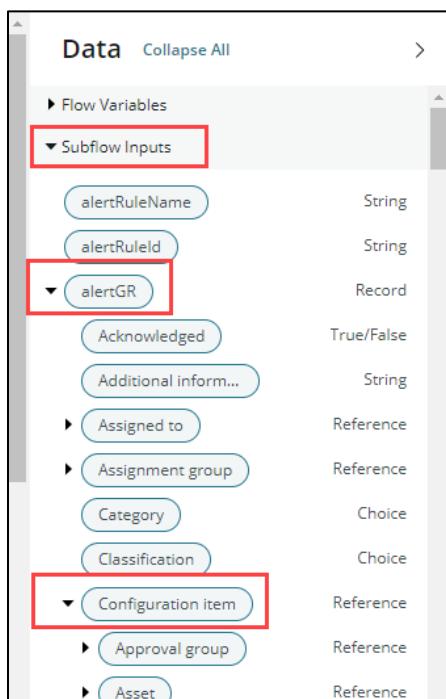
6. Hover over the host data pill to reveal the full path. Notice the FQDN comes from the configuration item record.



7. Click the X in the data pill to remove Fully qualified domain name.



8. In the Data pane, drill down to **Subflow Inputs > alertGR > Configuration item** and locate **IP Address**.



9. Click, hold, and drag the IP Address data pill into the **host** field.

Alert/Restart Service

Action: Stop/Start/Restart Service

* host: IP Address

vcName: Scripted (Expand to edit)

* action: restart

Buttons: Delete, Cancel, Done

Configuration Item Fields:

- First discovered
- Fully qualified ...
- GL account
- IP Address
- Install Status
- Installed
- Invoice number
- Justification
- Lease contract

A Input > alertGR > Configuration item > IP Address

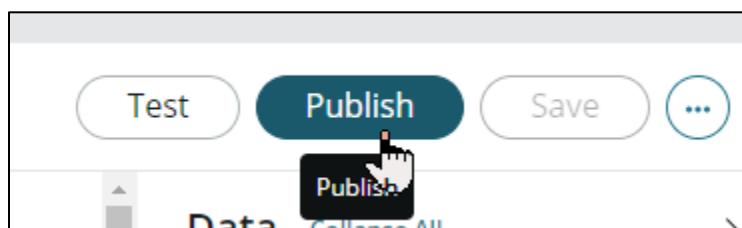
* host: Input > ... > IP Address (+x) X

* svcName: Scripted (Expand to edit)

10. In the Actions area, click **Done**.



11. In the menu bar, click **Publish**.



12. Return to **Service Operations Workspace** and open (if not already) the previous alert (print spooler).

13. On the Playbook tab, click **Restart Windows Service**.

The screenshot shows the ServiceNow interface with the 'Playbook' tab selected. A red box highlights the 'Playbook' tab in the top navigation bar. Below it, there are two cards representing actions:

- Action: Get Windows Processes**
- Action: Restart Windows Service**
 - Last executed at 2023-01-31 00:01:55
 - A 'Restart Windows Service' button is shown with a hand cursor icon, indicating it is clickable.

14. Wait for the action to complete.

A green success message box displays the text: "Restart Windows Service executed successfully".

15. Scroll down to see you can click on a link to the Flow Designer execution for troubleshooting (opens in a new tab).

The screenshot shows the 'Last executions' list. A red box highlights the 'Link to execution' column for the 'Restart Windows Service' row. A hand cursor icon is positioned over the link, which is labeled: [/_\\$flow-designer.do?sysparm_nostack=true](#).

16. On the alert **Details** tab, review the Activity section. Remediation results are displayed here. Click **Show more**.

Details Related records Metrics Playbook

Post Work notes (Private)

Activity

Status	Name
Running	Spooler

Show more

Note: If not shown after a few minutes, refresh the browser tab.

Activity

System Administrator
Work notes • 2023-05-24 20:55:43

Service request results:

Status	Name	DisplayName	PSComputerName
Running	Spooler	Print Spooler	198.51.65.29

Restarted service: Print Spooler

Show less

G. Challenge Lab: Modify Get Windows Services.

CHALLENGE

Return to Flow Designer subflows and modify the **Get Windows Services** to also use IP address instead of FQDN. Save and Publish. Return to the alert Playbooks tab and click **Get**

Windows Services. The result in the Details tab should look like this:

The screenshot shows the ServiceNow Details tab for a Windows service. The top navigation bar includes 'Details', 'Related records', 'Metrics', and 'Playbook'. The main area displays a summary card with the following information:

- Created: 2023-01-25 22:16:38
- Last modified: 2023-01-25 22:16:47
- Generation time: 2023-01-30 20:03:30

A section titled 'Information' contains the word 'okdown'.

To the right, a yellow sidebar for 'System Administrator' shows the following table of services and their statuses:

Status	Name	DisplayName
Running	AgentClientColl...	Agent Client Coll...
Stopped	AJRouter	AllJoyn Router Se...
Stopped	ALG	Application Layer
Running	AmazonSSMAgent	Amazon SSM Agent
Stopped	AppIDSvc	Application Ident
Running	Appinfo	Application Infor...
Stopped	AppMgmt	Application Manag...

17. **PLEASE READ:** The next lab has you load demo data which can take 20 minutes to settle in and stabilize. Depending on your schedule, you may want to continue to the next lab and complete section A to load the demo data, then return to the next lesson.



Congratulations on completing the lab!

Alerts and Tasks

Configure the Service Map

Lab
4.3
20m

Lab Objectives

You will achieve the following objectives:

- Configure alert impact settings
- View alert impact trees

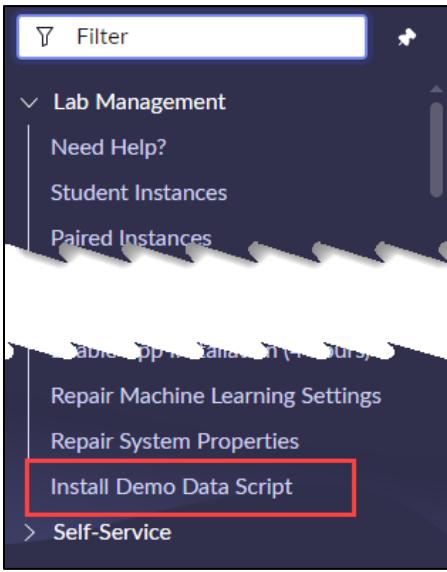
Scenario

In this lab, we load Service Mapping and Event Management plugin demo data, which includes application services and alerts that impact them. We will use an application service that includes clusters and modify the impact influence of the cluster members, maintaining the health of the overall application service when just one cluster member is critical.

As part of the student instance created for you, a non-standard link runs a script that loads the demo data. Demo data can be loaded in your own non-production instance from the plugin repair menu.

A. Load demo data for SM and EM

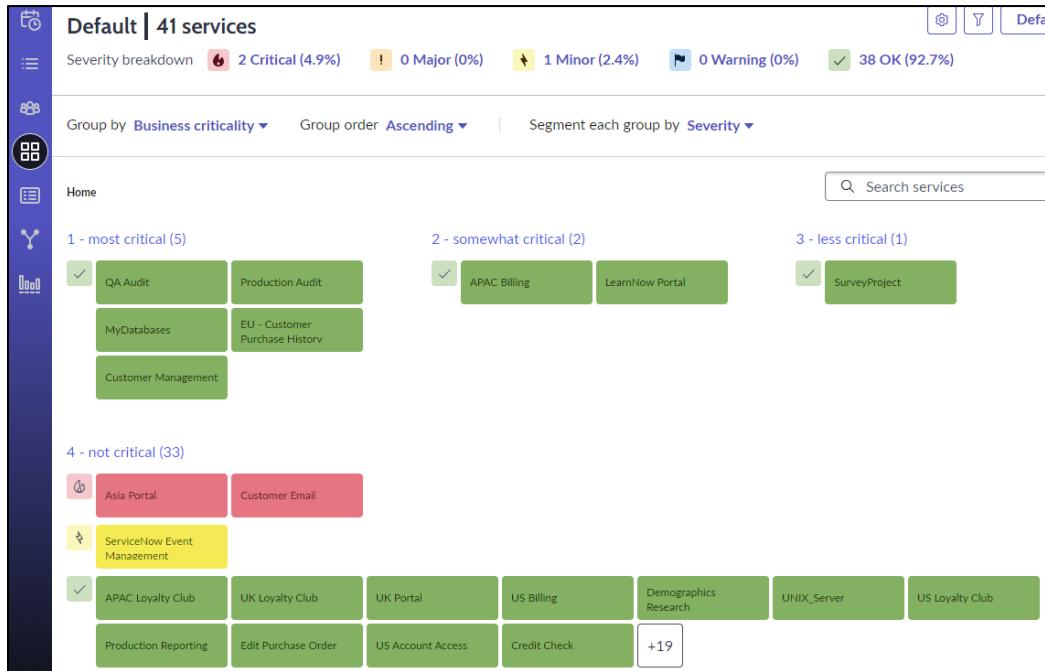
1. Navigate to and click **Lab Management > Install Demo Data Script**. The workspace may go blank.



2. The installation takes about four minutes. Wait for it to complete.

```
[0:02:30.902] Script completed in scope global: Install Demo Data Script
Script execution history available here
Loading: change_request.xml from unload.demo
[CacheFlushLog] event=wf_workflow_version, count=1, ms=0: Flushing catalog wf_workflow_version
[CacheFlushLog] event=WORKFLOW_VERSION_DATA_CACHE, count=1, ms=1: Flushing catalog WORKFLOW_VERSION_DATA_CACHE
[CacheFlushLog] event=WF VERSIONS FOR TABLE, count=1, ms=1: Flushing catalog WF VERSIONS FOR TABLE
[CacheFlushLog] event=workflowModel_cache, count=1, ms=1: Flushing catalog workflowModel_cache
Loaded: 1 rows into: change_request
Total rows loaded: 1
Loading: cmdb.xml from unload.demo
[CacheFlushLog] event=cmdb_ci_computer, count=1, ms=1215: Flushing catalog cmdb_ci_computer
[CacheFlushLog] event=cmdb_ci_spkg, count=1, ms=213: Flushing catalog cmdb_ci_spkg
[CacheFlushLog] event=cmdb_ci_rack, count=1, ms=300: Flushing catalog cmdb_ci_rack
[CacheFlushLog] event=cmdb_ci_web_server, count=1, ms=960: Flushing catalog cmdb_ci_web_server
```

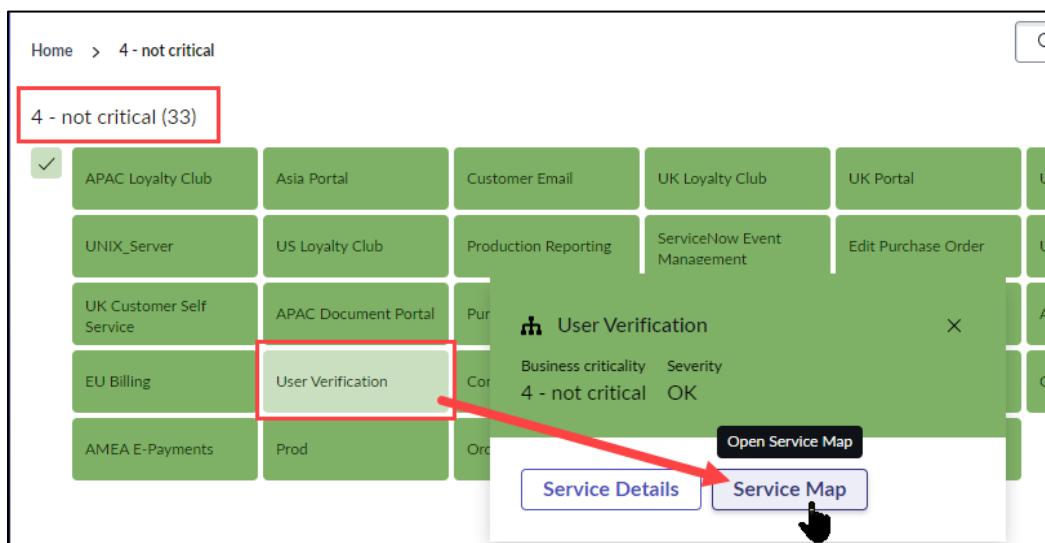
3. Verify demo data has loaded by opening the Service Operations Workspace service dashboard. A larger set of services is displayed with demo alerts. The alerts will be processed in the next few minutes and reflect impact.



Note: A great deal of processing occurs after the demo data loads and may take up to 20 minutes to stabilize in SOW. If the impact tree and controls are not showing, you may need to wait a few minutes more. The not-critical User Verification application service should be green.

B. Observe the Impact Configuration of the User Verification Service

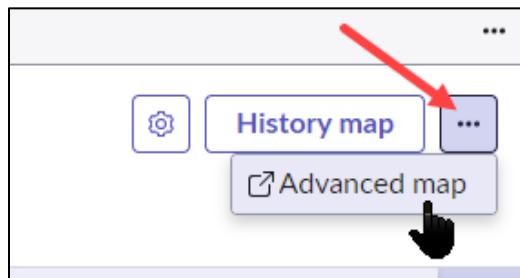
1. In Service Operations Workspace, open the **User Verification** service map.



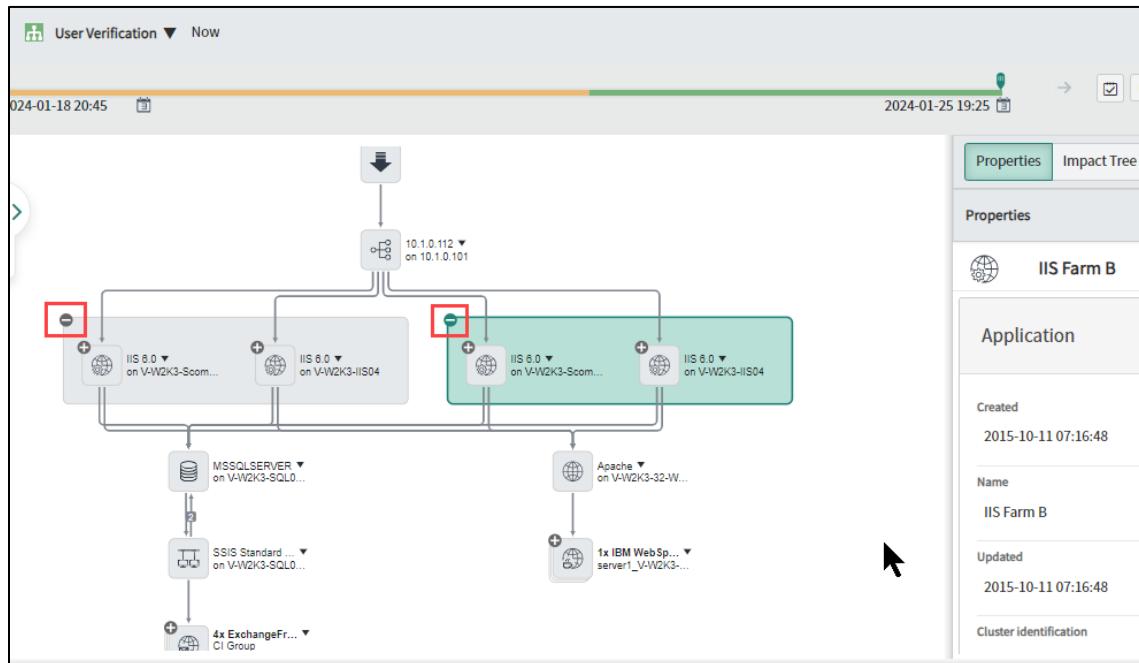
Note: If the User Verification tile is not shown, navigate to **Event Management > Services > Application Services**. Locate **User Verification** in the list, toggle the **Operational status** to non-operational, wait a few seconds, and then return to operational.

Name	Severity	Business criticality	Operational status	Service Type
User Verification	Clear	1 - most critical	Non-Operational	Discovered
US Loyalty Club	OK	4 - not critical	Operational	Discovered
US Billing	OK	4 - not critical	Non-Operational	Discovered
US Account Access	OK	4 - not critical	Repair In Progress	Discovered
UNIX Server	OK	4 - not critical	DR Standby	Discovered

2. In the upper right, click **Advanced Map**, which opens in a new tab.

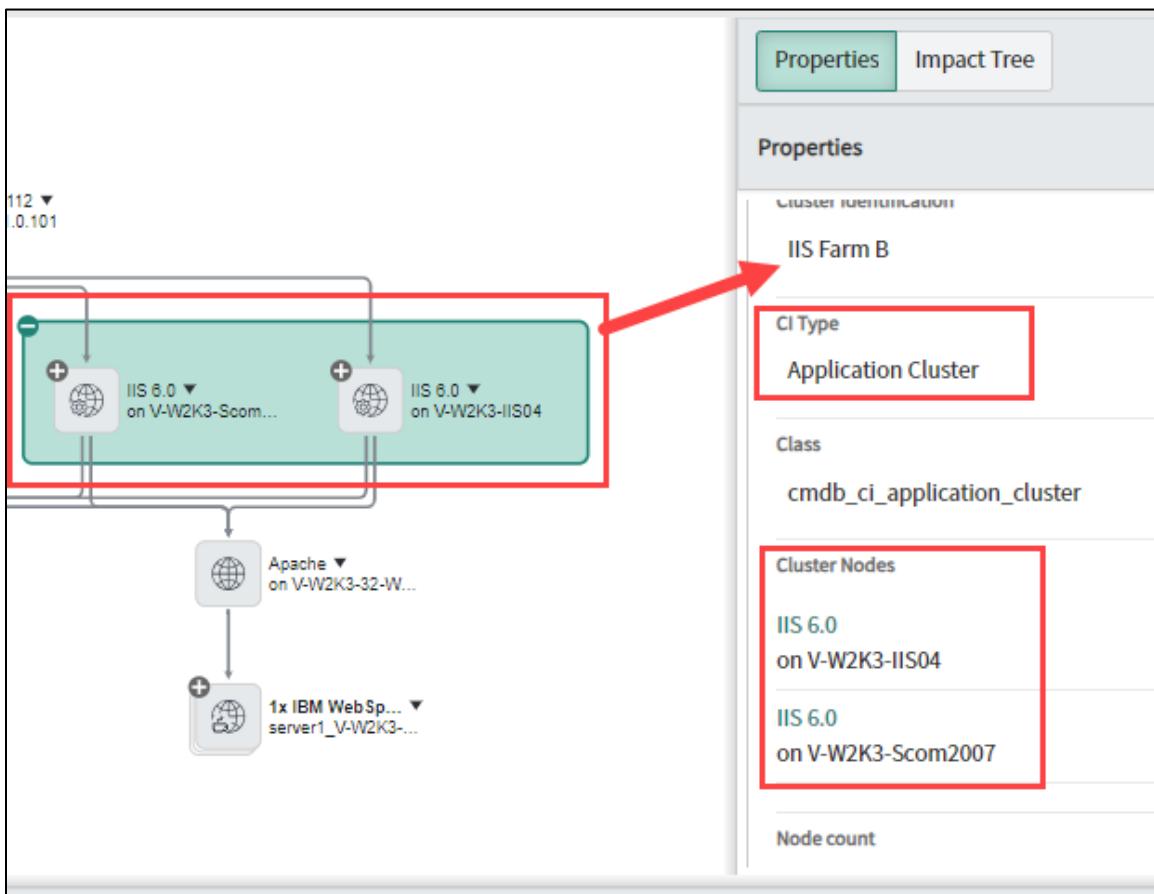


3. Click **+** to expand the two clusters, LoadBalancer240 and IIS Farm B.

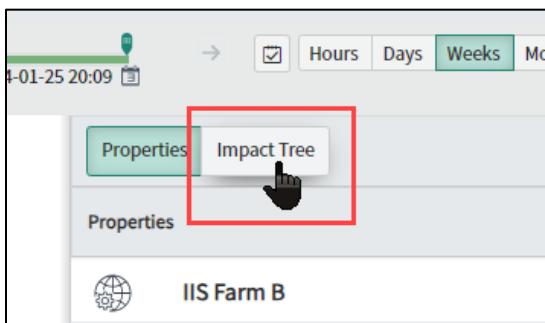


Note: The two clusters are supported by the same set of Windows Servers. Alerts bound to the server CI will impact both clusters. We will modify the impact settings of IIS Farm B, which will allow a comparison of the impact propagation between the modified and unmodified clusters.

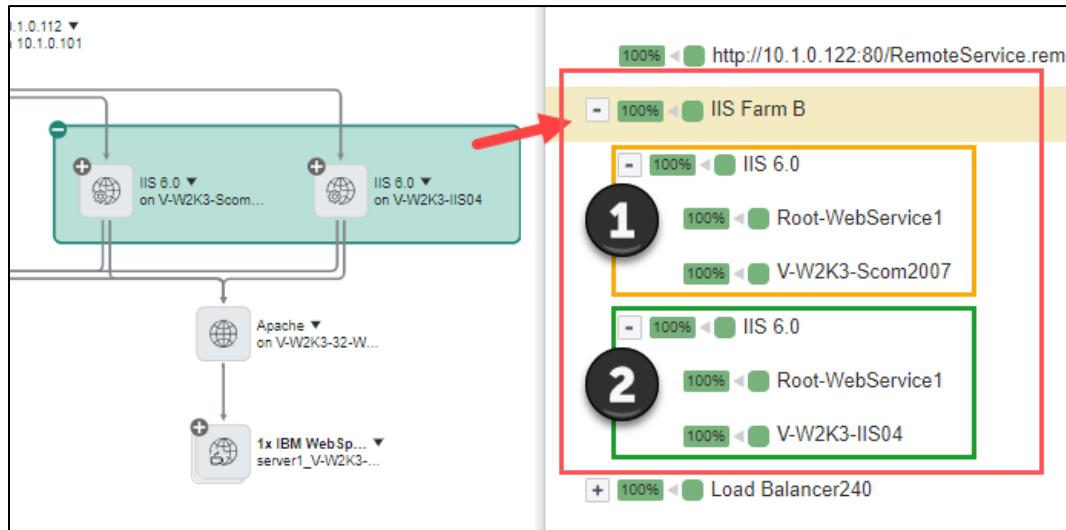
- With the IIS Farm B cluster selected, review the Properties frame.



- Click **Impact Tree**.

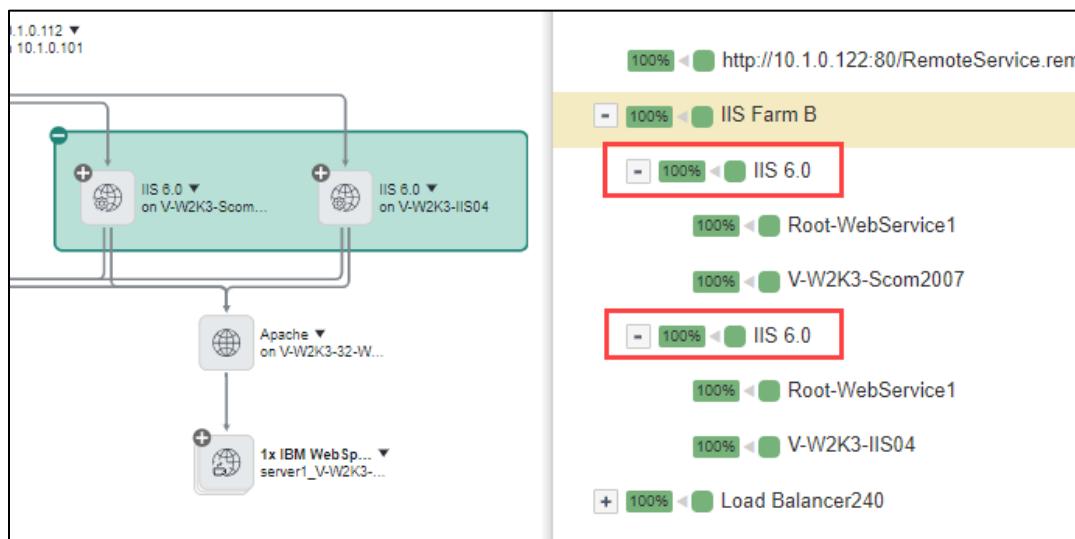


- Click to expand each component of the IIS Farm B cluster. The two cluster members each have a web service running on a server.



Note: If the impact tree does not display, skip to the Impact step below and continue. The tree will re-paint after the impact influence is changed.

7. You can click items in the list to see them on the map and click items on the map to see them in the list.
8. With the **IIS Farm B** selected, review the % impact each cluster member (IIS 6.0) has on the overall cluster health (100%) based on the current impact settings.



Note: Because this is a 2 member cluster, each cluster member has a **fixed** 50% influence on the overall cluster health. In a 4-member cluster each member would have 25%, and in a 5-member cluster 20%.

C.Modify the Impact Definition with Units

Modify the cluster member impact definition so that a single member outage does not reflect in the parent cluster or the application service.

1. Click **Impact** at the bottom.



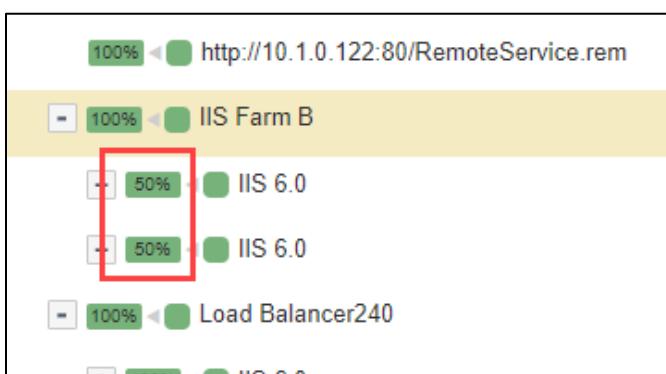
2. Configure the **Application Cluster Member** so that each member has a 50% influence threshold on the parent cluster using **Unit**.

- Influence **2**
- Influence Units **Unit**

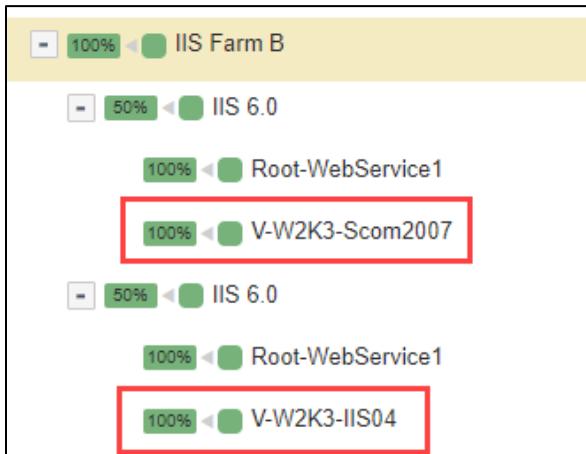
Name	Impact On	Influence	Influence Units	Critical
Application Impact	Application Service	100	Percent	<input type="checkbox"/>
Application Cluster Member	Parent	2	Unit	<input type="checkbox"/>

Note: Tab or click out of the fields after changing them then wait a few seconds for the impact tree to update. Setting Influence to 2 units means that 2 members need to be critical in order for the parent cluster to show critical.

3. The impact tree will update to 50% influence threshold for each member (IIS 6.0). By selecting 2 Units of impact in a 2-member cluster, each member now has a 50% influence on the parent cluster.



4. On the impact tree with the cluster members (IIS 6.0) expanded, observe the host server CI has a 100% influence on the cluster member.

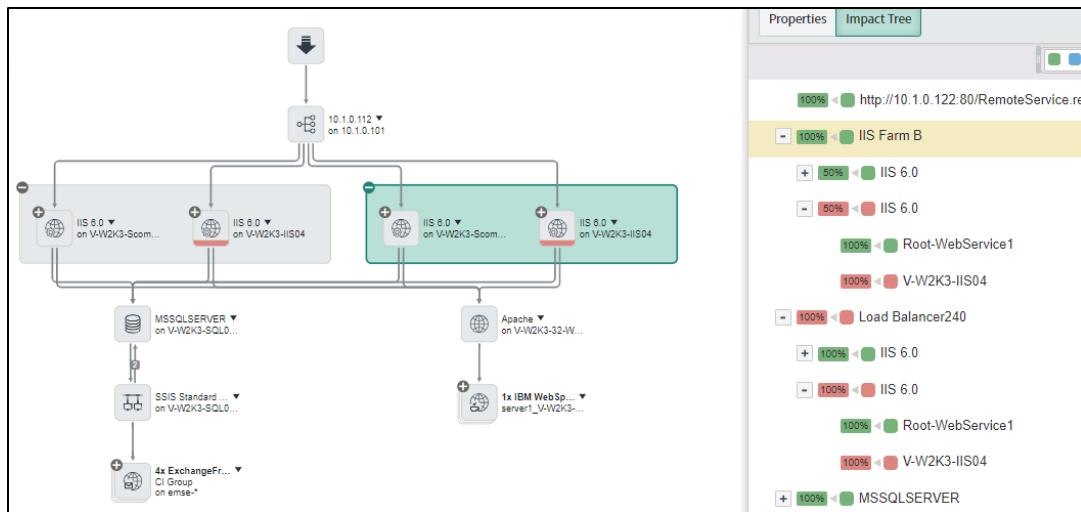


D. Generate Critical Event Against the User Verification Application Service

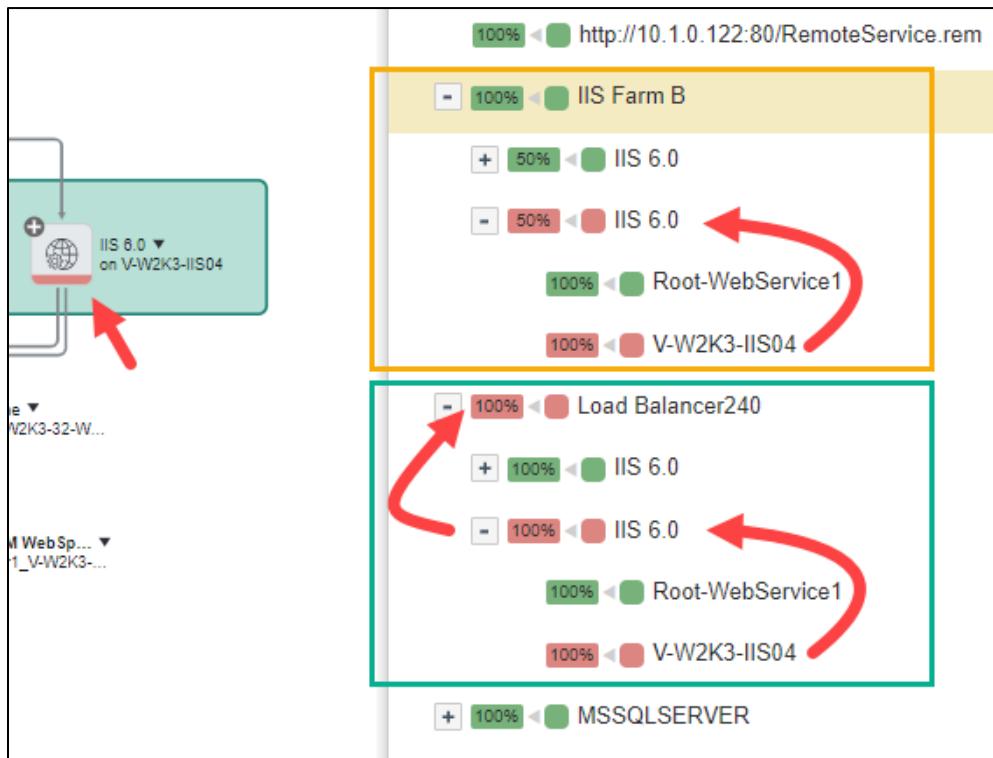
1. Switch to the instance tab. Load and fire the **Lab4.3 Critical Server Error** sample event.

```
source: PSScript
node: V-W2K3-IIS04
severity: Critical (1)
description: Spectrum: RadWare CHASSIS DOWN
type: SNDemo
source instance: PS
```

2. Return to the Advanced Map browser tab and wait a few seconds for the maps to update. When the alert is processed and impact calculated, the impact tree colors will change.



3. Review the Impact Tree.



Note: The V-W2K3-IIS04 server supports 1 cluster member in each cluster (IIS Farm B and Load Balancer240). The cluster members (IIS 6.0) show critical (red). Because of the impact change made to IIS Farm B, IIS Farm B does not show critical (green). Notice cluster Load Balancer240 does show critical (red) because its cluster members have 100% impact on the parent cluster.

4. Scroll up to the top of the **impact tree**.

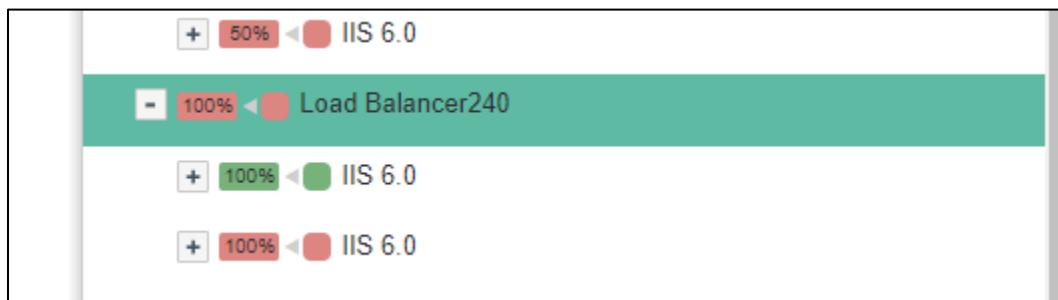


Note: Because the Load Balancer240 cluster is critical, the application service User Verification shows critical. The application service should not display critical, as it is fully functional.

E. Modify Impact Definition to Propagate a Different Severity

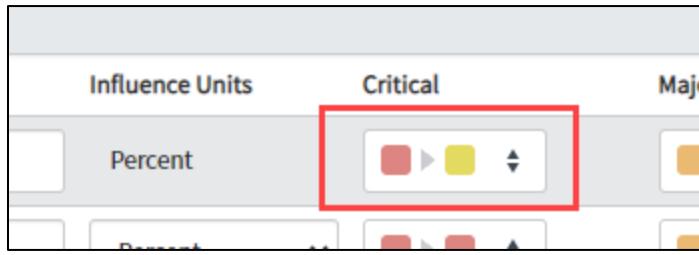
In this instance, where a single cluster member is critical but the application service is not effected, we can change the impact definition to show a less-than-critical impact on the parent cluster and service.

1. In the impact tree, select the Load Balancer240 cluster.

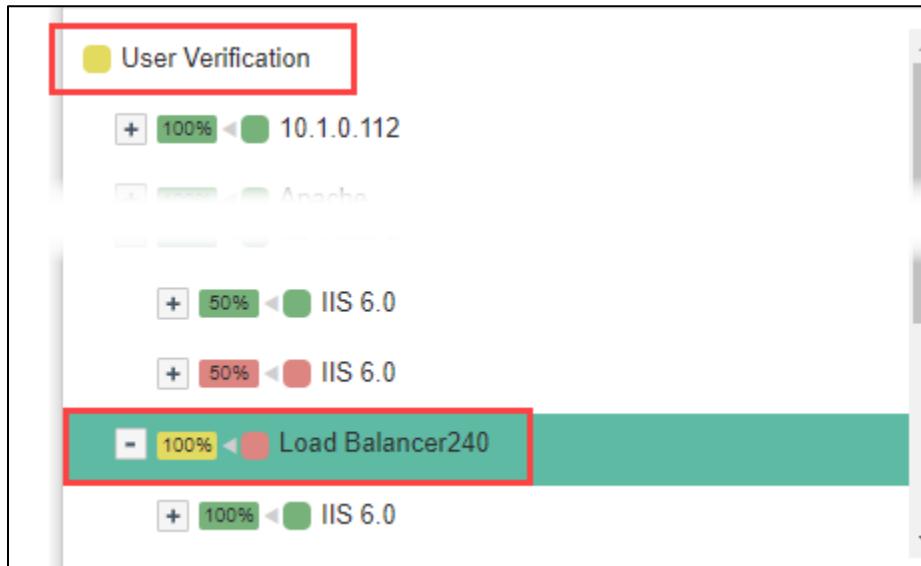


2. In the bottom Impact pane, modify the Application Impact critical alert color bar to propagate **minor**.

A screenshot of the 'Impact' pane. The 'Impact' tab is selected. A row for 'Application Impact' is highlighted with a red box. The 'Impact On' dropdown is set to 'Application Service'. The 'Influence' input field is set to '100' and 'Percent'. The 'Influence Units' dropdown is set to 'Percent'. To the right of the influence units, there is a color bar selector with a red arrow pointing to it. The color bar has several colored squares: red, yellow, green, blue, and orange. The red square is at the top. A small red box highlights the color bar's dropdown menu. The background of the pane is white.



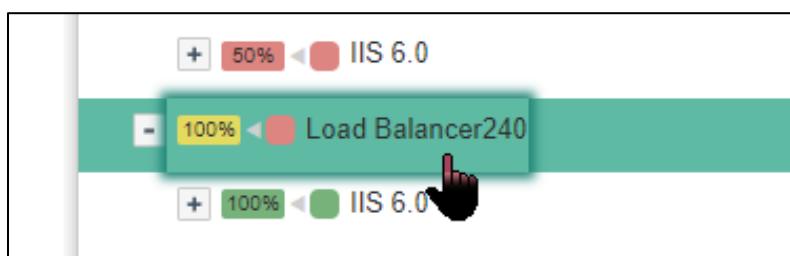
3. Wait for the tree to update. Both the parent cluster and the application service now reflect minor.



F. Modify the Impact Definition with Percent

Modify the Load Balancer240 impact definition using the percent units to respond as the IIS Farm B is.

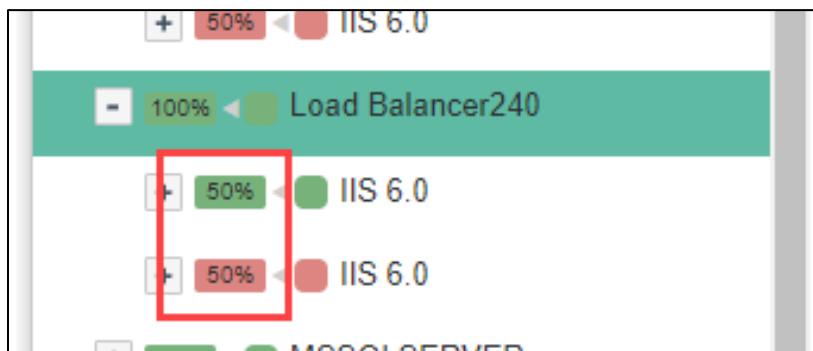
1. Configure the Load Balancer240 cluster members to also have a 50% impact on the cluster. In the impact tree, select the Load Balancer240 cluster.



2. In the bottom Impact pane, change the **Influence** to **51**. Leave units as Percent. Tab out of the fields.

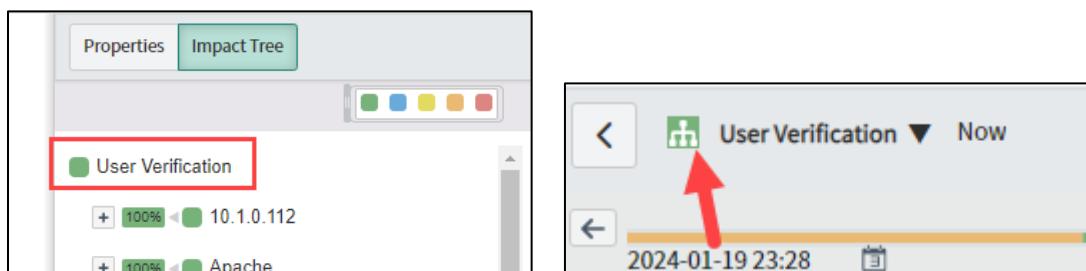
Alerts	Impact	Changes		
Name	Impact On	Influence	Influence Units	Criticality
Application Impact	Application Service	100	Percent	
Application Cluster Member	Parent	51	Percent	

3. Review the impact tree.



Note: The Load Balancer240 cluster members now each have a 50% impact on the parent cluster health, after setting the influence threshold to 51, which is above the 2 member cluster fixed influence of 50%.

4. Scroll to the top of the impact tree to see the application service User Verification has returned to green.



Note: The impact of the Windows cluster members is no longer large enough to change the color on the parent cluster and therefore there is no impact on the application service.

Congratulations on completing the lab!

Alerts and Tasks

Application Service SLAs

Lab
4.4
15m

Lab Objectives

You will achieve the following objectives:

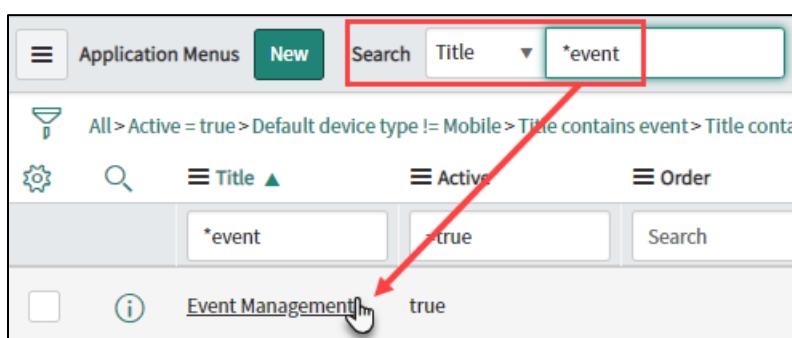
- Configure service level agreements (SLAs)

Scenario

In this lab, business service SLAs track critical alerts causing outages for the Survey Project application service. Create a new application navigator menu item to simplify tracking of application service SLAs (tasks). Then create an SLA definition and fire an event that starts the clock.

A. Event Management SLA Module Creation

1. Navigate to **System Definition > Application Menus**.
2. Locate and open **Event Management**.



3. From the **Modules** related list, create a **New** module as shown:

- Title: **Event SLAs**
- Application menu: **Event Management**
- Order: **27**
- Link type: **List of Records**
- Table: **Event Management SLA [em_ci_severity_task]**

Title: Event SLAs

Application menu: Event Management

Order: 27

Hint:

Display name:

Link Type: List of Records

Table: Event Management SLA [em_ci_severity_task]

4. Click **Submit**.
5. Click **Update** on the Application Menu.
6. Navigate to **Event Management > Event SLAs**.

Note: *This module was created in the previous steps.*

7. Observe the Event Management SLA for **Survey Project**.

Number	CI	Severity	Type
TASK0020121	ServiceNow Event Management	OK	Business Service
TASK0020122	LearnNow Portal	OK	Business Service
TASK0020123	SurveyProject	OK	Business Service
TASK0020413	Americas Calendar Portal	OK	Business Service
TASK0020430	MyDatabases	OK	Business Service

Note: *These SLAs generate when the application/business services are created. The records track the status of the application service. When alerts impact, the severity for the relevant service updates via a scheduled job running every minute.*

B. Configure an SLA Definition for Survey Project

1. Navigate to **Service Level Management > SLA > SLA Definitions**.

2. Create a new **SLA Definition** as shown:

- Name: **Survey Project SLA**
- Type: **SLA**
- Target: **Resolution**
- Table: **Event Management SLA [em_ci_severity_task]**
- Duration: **04 Days**
- Schedule: **24x7**
- Timezone source: **The SLA definition's time zone**

The screenshot shows the 'Create SLA Definition' form. The 'Name' field is 'Survey Project SLA'. The 'Type' dropdown is set to 'SLA'. The 'Target' dropdown is set to 'Resolution'. The 'Table' dropdown is set to 'Event Management SLA [em_ci_severity_task]'. The 'Duration type' is 'User specified duration', with 'Duration' set to 'Days 4'. The 'Schedule source' is 'SLA definition', and the 'Schedule' is '24 x 7'. The 'Timezone source' is 'The SLA definition's time zone'. The 'Application' is 'Global'. The 'Flow' is 'Default SLA flow'. The 'Enable logging' checkbox is unchecked. The 'Active' checkbox is checked.

Note: We are selecting 24x7 so that the clock runs in this example regardless of what time you are performing this lab. In production environments, choose the appropriate schedule.

3. Complete the **Start condition** tab as shown:

• Start condition:

- CI | is | SurveyProject AND
- Severity | is one of | Critical | Major

The screenshot shows the 'Start condition' tab. There are two conditions: 'CI | is | SurveyProject' and 'Severity | is one of | Critical | Major'. The 'Severity' dropdown is expanded, showing 'Critical', 'Major', 'Minor', and 'Warning'. 'Critical' and 'Major' are highlighted in blue. There are buttons for 'Add Filter Condition' and 'Add "OR" Clause'.

- Configure the **Stop condition** tab as shown:

- Stop condition: **Severity** | is | **OK**

The screenshot shows a search interface for 'Stop condition'. At the top, there are buttons for 'Stop condition', 'Add Filter Condition', and 'Add "OR" Clause'. Below these are three dropdown menus: 'Severity' (set to 'is'), 'is' (operator dropdown), and 'OK' (value dropdown). A 'Search' button is located at the bottom right of the search bar.

- Click **Submit**.

C. Generate a Survey Project Critical Alert

- Load and fire the **Lab4.3 SPServerError** sample event:

Source: **PSScript**
 Node: **198.56.1.200**
 Message_key: **4-3SP2017**
 Severity: **Critical (1)**
 Description: **Critical Issue on Server**
 Type: **SNDemo**

- Observe the new alert.

Number	Group	Severity	Created	Priority group	Priority	State	Source	Description
Search	Search	Search	Search	Search	Search	Search	Search	Search
Alert0010036		● Critical	2018-11-30 13:28:01	● High	2406	Open	PSScript	Critical Issue on Server

- Navigate to **Event Management > Event SLAs**.

- Observe the Survey Project SLA Severity is **Critical**.

Number ▲	CI	Severity	Type
TASK0020104	LearnNow Portal	OK	Business Service
TASK0020105	Survey Project	Critical	Business Service
TASK0020106	Americas Calendar Portal Manual	OK	Business Service

Note: It may take one minute to update the record from **OK** to **Critical**.

- Open the Survey Project SLA (i.e., click on the [TASKnnnnnnn](#) link).

The screenshot shows the 'Event Management SLA' screen for task TASK0020123. The SLA definition is set to 'Survey Project SLA' and 'SLA'. The 'Actual elapsed time' field is highlighted with a red box. The table below shows the SLA details:

SLA definition	Type	Target	Stage	Business time left	Business elapsed time	Business elapsed percentage	Start time
Survey Project SLA	SLA	Resolution	In progress	3 Days 23 Hours 59 Minutes	52 Seconds	0.02%	2022-07-11 16:58:45

Note: An active Task SLA is running against the Survey Project SLA. This is the SLA timer created based on the SLA definition created earlier. Your **Business elapsed time** may differ.

- Because of time and time zones, your Business elapsed time may differ or not start. To confirm progression of the SLA, add field **Actual elapsed time** to the list.

The screenshot shows the 'Task SLAs' list for task TASK0020240. The 'Actual elapsed time' field is highlighted with a red box. The table below shows the SLA details:

SLA definition	Type	Target	Actual elapsed time	Stage	Business time left	Business elapsed time
Survey Project SLA	SLA	Resolution	11 Minutes	In progress	4 Days	0 Seconds

D. Fire Clear Event Against Survey Project

- Load and fire the **Lab4.3 SPServerClear** event sample:

Source: **PSScript**
 Node: **198.56.1.200**
 Message_key: **4-3SP2016**
 Severity: **OK/Info (5)**
 Description: **Critical Issue on Server**
 Type: **SNDemo**

- View the alert.

	≡ Number	≡ Group	≡ Severity	≡ Priority group	≡ Priority	≡ State	≡ Source	≡ Description	≡ Node
	Search	Search	Search	Search	Search	Search	Search	Search	Search
Alert0010039			● OK	● Moderate	2406	Open	PSScript	Critical Issue on Server	198.56.1.200

Note: An event generates with a Severity of OK which clears the critical alert.

3. Navigate to **Event Management > Event SLAs**.
4. Observe the Survey Project SLA now has a **Severity of OK**.

Number ▾	CI	Severity
TASK0020121	ServiceNow Event Management	OK
TASK0020122	LearnNow Portal	OK
TASK0020123		OK
TASK0020413	Americas Calendar Portal	OK
TASK0020430	MyDatabases	OK

Note: It may take one minute to update from **Critical** to **OK**.

5. Open the **Survey Project Task** and scroll down to the Task SLAs section.

	Task SLAs	SLA definition	Search		Actions on selected r
TASK0020123					
	SLA definition	Type	Target	Actual elapsed time	Stage

Note: The Task SLA is now in a Completed stage. Had the alert not cleared in four days, then the Task SLA would be in a Breached stage.



Congratulations on completing the lab!

Event Sources

Create SolarWinds Connector

Lab
5.1
20m

Lab Objectives

You will achieve the following objectives:

- Create and test a SolarWinds connector
- Process events generated from the connector

Scenario

This lab involves creating and testing a SolarWinds connector on the 198.51 network. The training environment contains a SolarWinds server that is monitoring one Windows Server. The monitored server is configured to shut down for 3 hours daily, triggering a series of events.

Time of event ▾	Source	Description	Node	Type	Resource	Metric Name	N
2022-09-01 11:05:19	SolarWinds	Node ip-C6332FC8 has rebooted at Thursda...	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Alert Triggered	
2022-09-01 11:05:19	SolarWinds	ip-C6332FC8 rebooted at 9/1/2022 11:01:0...	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Node Rebooted	
2022-09-01 11:03:52	SolarWinds	Node ip-C6332FC8 is Up.	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Alert Reset	
2022-09-01 11:03:07	SolarWinds	ip-C6332FC8 is responding again. Respons...	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Node Up	
2022-09-01 08:04:07	SolarWinds	Node ip-C6332FC8 is Down.	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Alert Reset	
2022-09-01 08:04:02	SolarWinds	Node ip-C6332FC8 is Down.	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Alert Triggered	
2022-09-01 08:03:01	SolarWinds	ip-C6332FC8 has stopped responding (Host...	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Node Down	
2022-09-01 08:02:07	SolarWinds	Node ip-C6332FC8 is Warning.	198.51.47.200		198.51.47.200.ip-198-51-47-200.ec2.internal	Alert Triggered	

Event Management includes several connector configurations, such as event rules and field mappings, out-of-the-box to speed implementation. You should review baseline rules and field mappings for any baseline connector you are activating to understand what is preconfigured.

Integrations launchpad, part of the AIOps Experience store app for Service Operations Workspace, was released in August of 2023. Launchpad provides a streamlined experience for all connector configurations including pull, push, and custom (webhook). Launchpad or Event Management connector instances can be used for configuring connectors.

A. Create a SolarWinds Credential

1. Navigate to **Discovery > Credentials**.
 2. Click **New**
 3. Choose **Basic Auth Credentials**.
- Basic Auth Credentials**
4. Configure the **Basic Auth Credential** as shown:
- Name: **SolarWinds EM**
 - User name: **admin**
 - Password: **event@1ert**

The screenshot shows a web-based form titled "Basic Auth Credentials" with a sub-instruction "New record [Discovery view]". The form has three fields: "Name" containing "SolarWinds EM", "User name" containing "admin", and "Password" containing "event@1ert". The "Password" field is highlighted with a green border.

5. Click **Submit**.

B. Create a SolarWinds Connector

1. Navigate to Event Management > Integrations > Metric Sources.



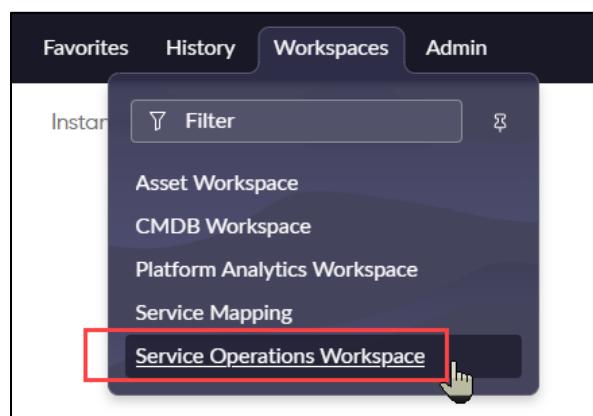
2. Locate the SolarWinds source and toggle Generate Missing CIs to True.

A screenshot of the 'SA Metric Type Registrations' table. The table has columns: Source, Registration Mode, Type default mode, and Generate Missing CIs. There are five rows: 'SNMPV2 Generic Trap' (Source: 'SNMPV2 Generic Trap', Registration Mode: Inactive, Type default mode: Inactive, Generate Missing CIs: false), 'SolarWinds' (Source: 'SolarWinds', Registration Mode: Inactive, Type default mode: Inactive, Generate Missing CIs: false), 'Splunk' (Source: 'Splunk', Registration Mode: Inactive, Type default mode: Inactive, Generate Missing CIs: false), 'Trap From Enterprise 9' (Source: 'Trap From Enterprise 9', Registration Mode: Inactive, Type default mode: Inactive, Generate Missing CIs: false), and 'vmwVC' (Source: 'vmwVC', Registration Mode: Inactive, Type default mode: Inactive, Generate Missing CIs: false). A red arrow points to the 'Generate Missing CIs' dropdown for the 'SolarWinds' row, which is currently set to 'false'. A mouse cursor is hovering over the dropdown menu, which shows the options 'true' and 'false'.

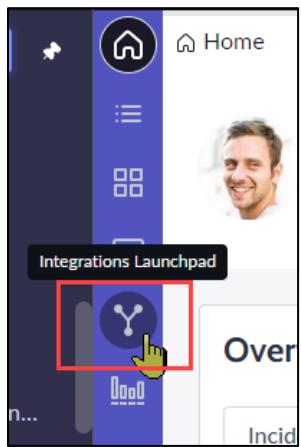
Source	Registration Mode	Type default mode	Generate Missing CIs
SNMPV2 Generic Trap	Inactive	Inactive	false
SolarWinds	Inactive	Inactive	false
Splunk	Inactive	Inactive	false
Trap From Enterprise 9	Inactive	Inactive	false
vmwVC	Inactive	Inactive	false

Note: By default, Generate Missing CIs is set to false as it could generate many and duplicate CIs. In this case, SolarWinds is only monitoring one server.

3. Navigate to Service Operations Workspace.



4. Open **Integrations Launchpad**.



5. Locate and click the Solarwinds tile.

A screenshot of the 'Integrations launchpad' page in the ServiceNow web interface. The page title is 'Integrations launchpad'. Below it, a subtitle reads 'Bring together all of the events, metrics and logs from your infrastructure and get insights into the unified system.' There are two tabs: 'Browse integrations' (selected) and 'Installed integrations'. A search bar and a dropdown for 'All integrations' are also present. The main area displays several tiles for different data sources. One tile for 'Solarwinds' is highlighted with a red box and a cursor is shown clicking on its 'Logs' section.

6. Complete the connector instance as shown:

- Connector name: **SolarWinds EM**
- Host IP: **198.51.98.70**
- Credential: **SolarWinds EM**

SolarWinds EM

Connector name *

SolarWinds EM

Description

Enter description

Host IP *

198.51.98.70

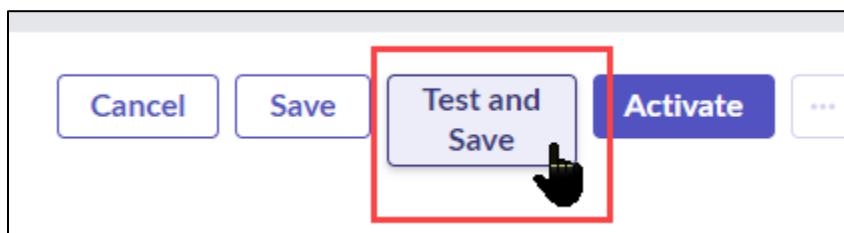
Credentials *

SolarWinds EM

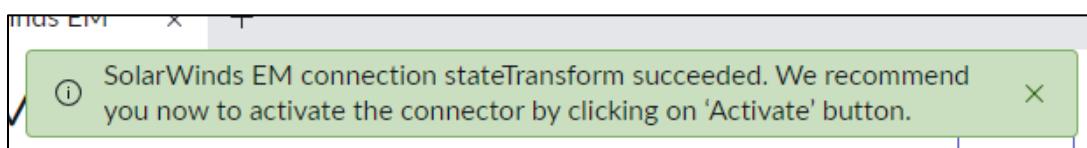
Advanced settings

Note: Advanced settings can be expanded and allows additional configuration such as selection of a specific MID Server or a different event collection schedule (default 120 seconds), as well as event collection status and error messages.

7. Click **Test and Save**.



8. Within a few seconds a success message should appear briefly.



9. Click **Activate**.

Note: MID Server certificate check policies (MID Security Policy) are enabled by default and will prevent MID to server connections unless the server certificate is added to the MID Server truststore. See documentation page "Add SSL certificates for the MID Server." The default policy has been disabled in this training environment.

10. Wait approximately 100 seconds, then in **All Events** observe the events collected from the **SolarWinds** source. "Show matching" on source = SolarWinds then sort by most recent on top.

Events						
		Source	Description	Node	Type	Resource
<input type="checkbox"/>		Time of event	=SolarWi	<input type="button" value="Search"/>	<input type="button" value="Search"/>	<input type="button" value="Search"/>
2024-06-06 08:01:50	SolarWinds		Agent ip-C6332FC8 became unavailable			
2024-06-05 08:01:44	SolarWinds		Agent ip-C6332FC8 became			

Note: The **Time of event** is the actual time the monitored Windows Server shut down/started up, not the current time of connecting and ingesting these events. For this reason, you may need to filter the Events list to locate the SolarWinds source events.

11. Open the SolarWinds event with **description** “Node ip-C6332FC8 is Down” and **metric name** “Alert Triggered” and observe the data collected.

2022-09-01 08:04:07	SolarWinds	Node ip-C6332FC8 is Down.	198.51.47.200	198.51.47.200,ip-198-51-47-200.ec2.internal	Alert Reset
2022-09-01 08:04:02	SolarWinds	Node ip-C6332FC8 is Down.	198.51.47.200	198.51.47.200,ip-198-51-47-200.ec2.internal	Alert Triggered
2022-09-01	SolarWinds	ip-C6332FC8 has stopped	198.51.47.200	198.51.47.200,ip-198-51-47-200.ec2.internal	Node Down

12. Review the **processing notes** to understand how the alert was populated. Notice the “Solarwinds Node Status” event rule applied. Also notice there is no Status field in the event.

Processing Notes	Event rule applied: Solarwinds Node Status Mapping rule(s) applied: solarwinds-type, solarwinds-icon-severity, solarwinds>Status-severity Alert is already bound to CI with id: 03ccb80b342a02107f443898a17bf671 Mapping rule(s) applied after binding: Alert Tags t_location-CMDB CI Value Based, Alert Tags t_i
------------------	--

13. Navigate to **Event Management > Rules > Event Rules** and open the **Solarwinds Node Status** rule.

14. On the rule's Transform and Compose tab, note how the description is used to derive the Node and Status fields.

Transform and Compose Alert Output

The screenshot shows the 'Transform and Compose Alert Output' interface. On the left, there is a list of fields with their current values:

- Description: \${description}
- Node: \${node}
- Type: \${type}
- Resource: \${resource}
- Message key: \${netObjectId}_\${networkNodeId}_nodeStatus
- Severity: \${severity}
- Metric name: \${metric_name}
- Source instance: \${event_class}
- Source: \${source}
- Classification: \${classification}
- Additional information: \${Status}

On the right, there is a vertical sidebar labeled 'Event Input' containing buttons for various event types and details:

- Expressions
- Node
- Status
- Event Raw Info
- Descri...
- Node
- Type
- Resource
- Messa...
- Severity
- Metric ...
- Source...
- Source

Original field is: **Description**

Mark or edit string to turn it into a regex expression under Transform Data

Write Regex	Expressions
Node ([^']+)+ is (.+)\.	Node
	Status

The screenshot shows a 'REGULAR EXPRESSION' input field containing the pattern: `^Node\.([^]+)\.is\.(.+)\.`. Below it, a 'TEST STRING' input field contains the string: `Node.ip-C6332FC8.is.Down.`. The word 'ip' is highlighted in green, and 'Down' is highlighted in orange, demonstrating how the regex matches specific parts of the string.

Note: This graphic (above) is from the web site [regex101.com](https://www.regex101.com), which may be useful in creating and reverse engineering your regex expressions. Shown here to see how the expression will act on the event description.

15. Return to the event (hint: use History). Open the associated **Alert** and view the Activities tab to see how mapping rules were applied. NOTE THE ALERT NUMBER.

Note: Following screenshots and data may vary depending on the time of day you perform these steps. In most cases, the monitored server will be back up and the alert will have closed, with later events updating the alert information. The Configuration item may or may not be populated.



Number	Alert0010045	Severity	Major
Source	SolarWinds	State	Open
Node	ip-C6332FC8	Acknowledged	<input type="checkbox"/>
Type	Alert Triggered	Maintenance	<input type="checkbox"/>
Resource		Updated	2018-11-30 13:56:50
Configuration item		Parent	
Task		Knowledge article	
Metric Name		Overall Event Count	5
Description	Node ip-C6332FC8 is Down.		

Oping History Activities More Information Repeated Alerts Similar Alerts CI Incidents

Work notes Work notes

Activities: 2

System
Updated alert state from Open to Closed due to [event](#): Node ip-C6332FC8 is Up.

System
Created new alert with state Open due to [event](#): Node ip-C6332FC8 is Down.
Event rule applied: Solarwinds.Node.Status
Mapping rule(s) applied: [solarwinds-type](#), [solarwinds-icon-severity](#), [solarwinds>Status-severity](#)

Note: The solarwinds>Status-severity is the last mapping rule applied. The rule maps "Down" to severity "Major." This is a down node. The severity should be critical.

C.Modify the Severity of a SolarWinds Alert Field Mapping

Shown below are the baseline SolarWinds event field mappings in priority order. You can view these in your instance, along with several SolarWinds event rules. Notice there are four possible event fields that can be mapped to severity. All will be processed, and the last one to process “wins” the populating of the severity field.

Name	Order ▾	Source	From field	Mapping type	To field
solarwinds-type		SolarWinds	eventType	Single field	type
solarwinds-icon-severity	100	SolarWinds	icon	Single field	severity
solarwinds-Availability-severity	110	SolarWinds	Availability	Single field	severity
solarwinds-ComponentStatus-severity	120	SolarWinds	ComponentStatus	Single field	severity
solarwinds-Status-severity	130	SolarWinds	Status	Single field	severity

1. Navigate to **Event Management > Rules > Event Field Mapping**.
2. Locate and open the **solarwinds-Status-severity** rule.

All > Name contains Solarwinds	Name ▾	Active	Source	From field	Mapping type	To field
	<input type="checkbox"/> <input type="radio"/> *Solarwinds	<input type="checkbox"/> Search				
	solarwinds-Availability-severity	true	SolarWinds	Availability	Single field	severity
	solarwinds-ComponentStatus-severity	true	SolarWinds	ComponentStatus	Single field	severity
	solarwinds-icon-severity	true	SolarWinds	icon	Single field	severity
	<input checked="" type="radio"/> solarwinds-Status-severity	true	SolarWinds	Status	Single field	severity
	solarwinds-type	true	SolarWinds	eventType	Single field	type

3. From **Event Mapping Pairs**, next to the **Down Key**, change the **Value** to **1** (critical).

Event Field Mapping
solarwinds>Status-severity

Name: solarwinds>Status-severity Active:

Source: SolarWinds

Order: 130

Mapping type: Single field

From field: Status To field: severity

Event Mapping Pairs	
Key	Value
Up	5
Unmanaged	5
Warning	3
Critical	2
Down	1
Unknown	
Unreachable	

Note: In this mapping, the Down key returned from the Status field (attribute) sets a 2 (major) for the severity of the alert. Changing this value to 1 creates Critical alerts when the Status is Down and the Source is SolarWinds.

- Click **Update**.

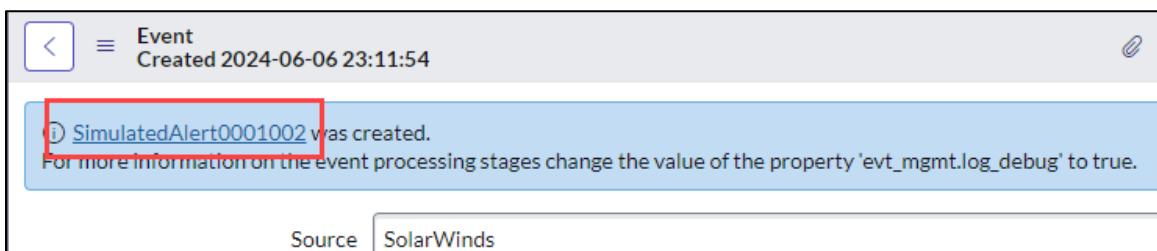
D. Test the Solution

- Navigate to All Events.
- Again locate the event with the **description** “Node ip-C6332FC8 is Down” and **metric name** “Alert Triggered.” The alert number should be the one noted earlier.

3. In **Related Links**, click **Simulate event processing**.



4. At the top of the event form, click the **simulated alert link**.



5. Processing with the updated mapping results in a critical alert.



Note: *Simulate event processing is a non-intrusive way to test your rules.*



Congratulations on completing the lab!

Event Sources

Processing Events from an Email Source

Lab

5.2

25m

Lab Objectives

You will achieve the following objectives:

- Process email events using a Flow Designer flow.

Scenario

A monitoring system is often configured to send emails when a significant event occurs. In this lab, you trigger an email to be processed to simulate this scenario. This email communication is processed by a custom flow converting the email into an event. Finally, an event rule is created to parse the event and generate an appropriate alert.

To trust and process incoming emails, ServiceNow needs a matching user and email address and a domain trust with the sending email domain. These email settings are preconfigured on your instance.

- User ID: monitor@acme.com
- Email: monitor@acme.com

A. Create a New Flow Designer Flow to Process Emails from This Monitoring Source

1. Navigate to **Process Automation > Flow Designer** which opens in a new tab.
2. On the **Flows** tab, click **New > Flow**.
3. The Flow Properties dialog box opens. Complete the form as shown:

- Flow name: **Process Email Event**
- Application: **Global**
- Protection: **None**
- Run As: **System User**

Properties

Flow name *

Description

Describe your flow.

Application *

Hide additional properties

Protection

-- None --

Run as

System user

Run with roles

Flow priority default

Medium (default)

4. Click **Build flow**.



5. In the **TRIGGER** section, click

6. Select **Application > Inbound Email** from the list.

Trigger

Search Triggers

Multiple	Action, Flow	Application
Record		Inbound Email
Scheduled		MetricBase
Application		Proactive Analytics
		Service Catalog
		SLA Task

7. Complete the **Email Conditions** as shown:

- **Subject** | starts with | **PSEmail** AND
- **User** | is | **monitor@acme.com**

The screenshot shows the 'Inbound Email' trigger configuration. Under 'Trigger', 'Inbound Email' is selected. Under 'Email conditions', the condition 'All of these conditions must be met' is displayed. A red box highlights the following two conditions:

- Subject starts with PSEmail
- User is monitor@acme.com

These two conditions are connected by an 'AND' operator.

8. Click **Done** to close the trigger section.



9. In the **ACTIONS** section, click

10. Click **Action**.

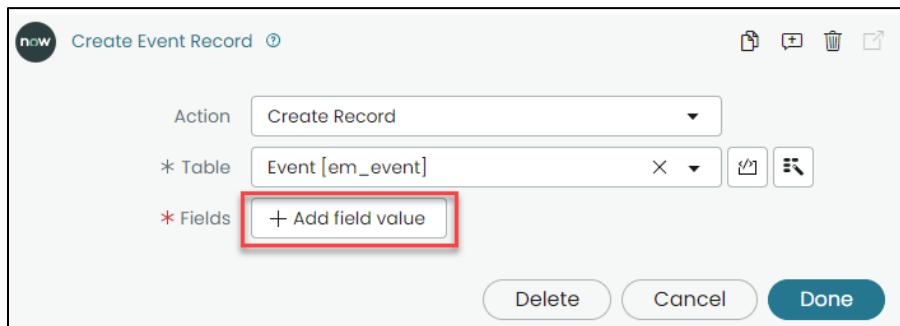
The 'ACTIONS' section contains three buttons: 'Action' (highlighted with a red box), 'Flow Logic', and 'Subflow'.

11. Select **ServiceNow Core > Create Record**.

The 'Search Actions' dialog is open, showing a list of actions. The 'ServiceNow Core' category is selected (highlighted with a blue box). Within this category, 'Create Record' is selected (highlighted with a red box and a hand cursor icon).

12. In the **Table** field, select **Event [em_event]**.

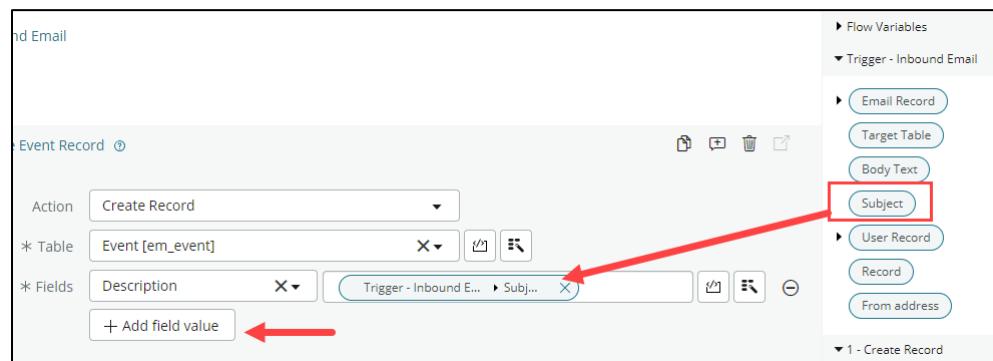
13. Next, add the fields you want mapped from the email to the event record. Click **+Add Field Value**.



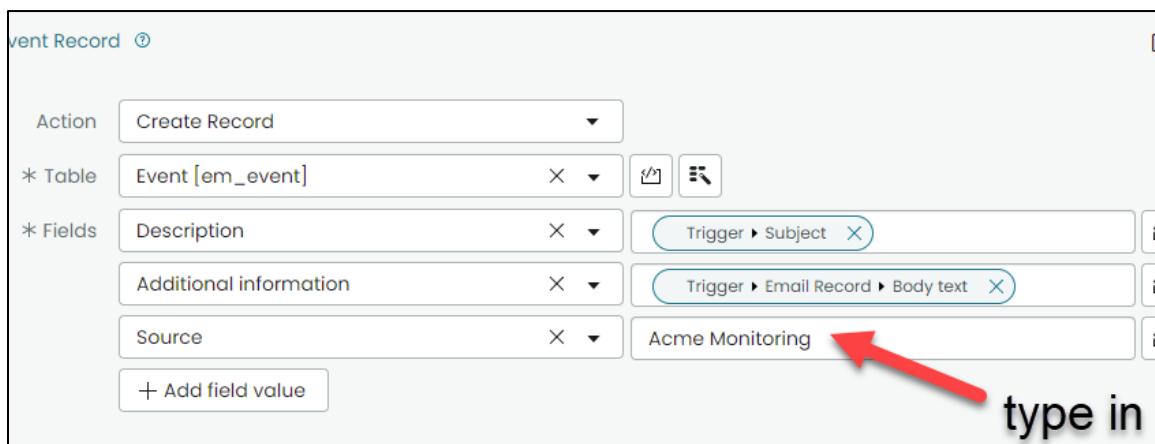
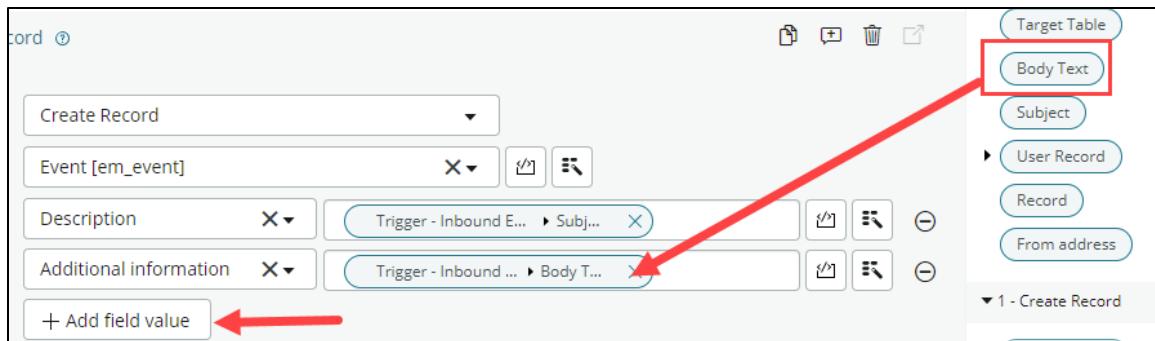
14. Complete the **Fields** section as shown: **Drag** the data pills from the right panel Data section to populate the form. Type in Acme Monitoring for Source.

Note: *Scroll down and look at the screenshots below to see what the result should look like!*

- Description: **Trigger – Inbound Email > Subject**
AND (+Add field value)
- Additional information: **Trigger – Inbound Email > Email Record > Body text**
AND (+Add field value)
- Source: **Acme Monitoring**



Note: *Expand **Email Record** and select the **Body text** data pill. Email records contain both "body" and "body_text" fields. Body is the HTML version of body_text. In our sample email, both fields contain the same data.*



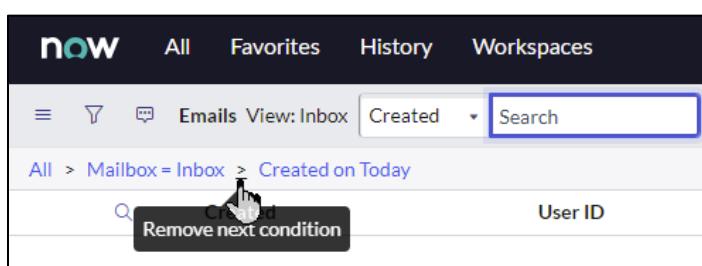
15. Click **Done** to close the Actions.

16. Click **Activate**, and **Activate** again to confirm.

17. Return to the instance tab and navigate to **System Mailboxes > Inbound > Inbox**.

Note: Our training instances are not connected to email servers, so an email has been prepopulated in the Inbox to be processed.

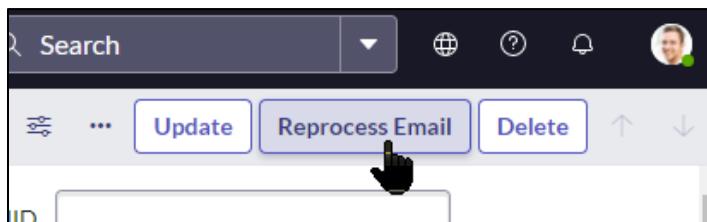
18. Remove the filter condition **Created on Today**.



19. Locate and open the email with **Recipients of monitor@acme.com**.

Emails View: Inbox				
Created		User ID	Recipients	Subject
2021-09-03 16:03:17	(empty)	monitor@acme.com	PSEmail: Error 198.56.1.201 not responding	Ignored

20. In the upper right, click Reprocess Email.



21. Navigate to All Events.

22. Locate and open the event just created with a Source of Acme Monitoring.

Events				
Time of event		Source	Description	Node
2022-07-15 18:33:20		Acme Monitoring	PSEmail: Error 198.56.1.201 not responding	
2022-07-15 17:01:33		PSScript	Critical Issue on Server	198.56.1.201

23. Review the fields mapped from the email.

Severity	-- None --
Resolution state	New
Time of event	2022-07-15 18:33:20
State	Error
Alert	
Description	PSEmail: Error 198.56.1.201 not responding
Additional information	[{"level": "1", "origin": "acme-server"}]
Error message	severity: Invalid value

Note: The data regarding the Severity and Node are embedded in the Description and Additional information. There is currently no Severity, so the event State is Error.

B. Configure an Event Rule to Process the Incoming Email Based Event

1. From within the open event, click **Create Event Rule**.
2. Complete the **Event Rule Info** as shown:

The screenshot shows the 'Event Rule Info' configuration page. At the top, there are two tabs: 'Event Rule Info' (which is selected) and 'Event Filter'. Below the tabs, the title 'Event Rule Info' is displayed. The configuration fields are as follows:

* Name	PSEmail - Lab
Source	Acme Monitoring
* Order	100
Description	(empty)

3. Configure the **Event Filter** as shown:

The screenshot shows the 'Event Filter' configuration page. The title 'All of these conditions must be met' is at the top. Below it, there are three conditions connected by 'AND':

- Description starts with PSE
- Classification is IT
- Description ends with not responding

4. From **Transform and Compose Alert Output**, under **Event Raw Info**, click **Description**.

Event Raw Info

Description	PSEmail: Error 198.56.1.201 not responding
-------------	--

- Highlight the IP address match it to **Node**.

Mark Expressions	Expressions
PSEmail: Error 198.56.1.201 not responding	Node X

- Click **Done**.

- Under **Event Additional Info**, drag **origin** to replace **Source \${source}** on the left.

Compose Alert fields by adding free text and by dragging variables from the right pane.
Click Event Raw values to create new regex expressions.

Description	<input type="text" value="\${description}"/>	Event Input
Node	<input type="text" value="\${node}"/>	level 1
Type	<input type="text" value="\${type}"/>	origin acme-server
Resource	<input type="text" value="\${resource}"/>	Expressions
Message key	<input type="text" value="\${message_key}"/>	Node 198.56.1.201
Severity	<input type="text" value="\${severity}"/>	Event Raw Info
Metric Name	<input type="text" value="\${metric_name}"/>	Desc... PSEmail: Error
Source instance	<input type="text" value="\${event_class}"/>	Node
Source	<input style="outline: 2px solid green; border: 1px solid green;" type="text" value="\${origin}"/>	Type
		Reso...
		Mess...

Note: If click and drag does not work from your system, you can simply type the value \${origin}.

- Drag **level** to replace **Severity \${severity}** as shown:

Message key	<code>\$(message_key)</code>
Severity	<code>\$(level)</code>
Metrics name	<code>\$(metric_name)</code>

9. Configure **Message key** as shown:

- Message key: `PSEmail_${origin}_${level}_${node}`

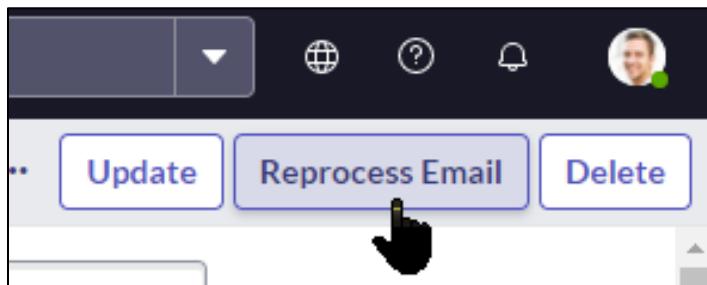
Message key	<code>PSEmail_\${origin}_\${level}_\${node}</code>
-------------	--

Note: There is no Message key sent from the event via email. Type in "PSEmail_" at the start of the field. Insert underscore character to separate the data.

10. Click **Submit**.

C. Send an Email Generating an Event and an Alert

1. From **Inbox**, locate and open the email with **Recipient** of `monitor@acme.com`.
2. In the upper right, click **Reprocess Email**.



3. Navigate to **All Events**.
4. Open the associated event and validate that the event rule was applied.

State	Processed
Alert	Alert0010031

Processing Notes Binding alert CI process flow: Node is IP address Node was not found, checking by name Event CI type is empty No CI found for binding (Failed to resolve the event node to CI id) Binding Failure Reason: Failed to find the host with name: 198.56.1.201	Event rule applied: PSEmail - Lab Not able to assign alert based on "cmdb_ci.support_group" since the alert is not bound to a CI Not able to assign alert based on the connectors assignment group ("IntegrationGroup") since the Source instance is empty
---	---

5. **Open** the associated alert.

Number	Alert0010055	Severity	Critical
Source	acme-server	State	Open
Node	198.56.1.201	Acknowledged	<input type="checkbox"/>
Type	<input type="text"/> <input type="button" value="🔍"/>	Maintenance	<input type="checkbox"/>
Resource	<input type="text"/>	Updated	2024-05-16 18:16:41
Configuration item	<input type="text"/>	Parent	<input type="text"/> <input type="button" value="🔍"/>
Task	<input type="text"/> <input type="button" value="🔍"/>	Knowledge article	<input type="text"/> <input type="button" value="🔍"/>
Metric name	<input type="text"/>	Overall Event Count	1
Description	PSEmail: Error 198.56.1.201 not responding		
Message key	PSEmail_acme-server_1_198.56.1.201		

Note: The alert is populated per the event rule.

6. Finally, **Close** the alert.



Congratulations on completing the lab!

Event Sources

Capture and Process SNMP Traps

Lab

5.3

30m

Lab Objectives

You will achieve the following objectives:

- Capture and process SNMP traps

Scenario

In this lab, we capture and process events from SNMP traps. You add an SNMP trap collector extension to your MID server, then use the preinstalled Gambit Communications MIMIC® Simulator to send SNMP traps. In a real-world scenario, monitoring systems in your infrastructure generate SNMP traps.

In this lab we will be using SNMP version “v1 and v2c.” Version 3 (v3) is recommended in production environments and requires additional security configuration, like credentials.

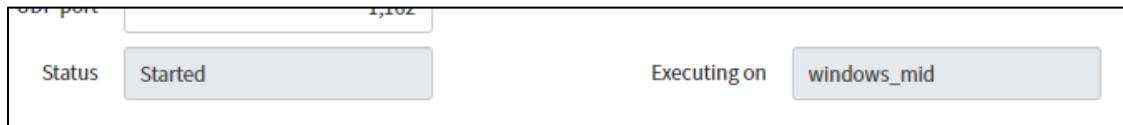
A. Create an SNMP Trap Collector Extension

1. In your ServiceNow instance, navigate to **Event Management > Integrations > MID SNMP Trap Listeners**.
2. Click **New** to create a new **SNMP Trap Collector Context** as shown:
 - Name: **SNMP Trap Collector EM**
 - UDP port: **1162**
 - Execute on: **Specific MID Server**
 - MID Server: **windows_mid**

The screenshot shows a 'Create New' dialog for an SNMP Trap Collector Context. The fields are as follows:

* Name: <input type="text" value="SNMP Trap Collector EM"/>	Execute on: <input type="text" value="Specific MID Server"/>
Short description: <input type="text"/>	* MID Server: <input type="text" value="windows_mid"/> <input type="button" value="Search"/> <input type="button" value="Help"/>
SNMP version: <input type="text" value="v1 and v2c"/>	
* UDP port: <input type="text" value="1162"/>	Status: <input type="text"/>
	Executing on: <input type="text"/>

3. From Additional actions, **Save**.
4. Under **Related Links**, click **Start**.
5. Reload the form until the **Status** changes to **Started**.



B. Access the MIMIC Simulator

In this section, you will log into your Windows server VM to configure and use the MIMIC Simulator to send SNMP traps.

You should already have your login information for your personal Windows server as provided in your instance registration in Now Learning.

1. Navigate to the remote desktop application on your laptop/computer.

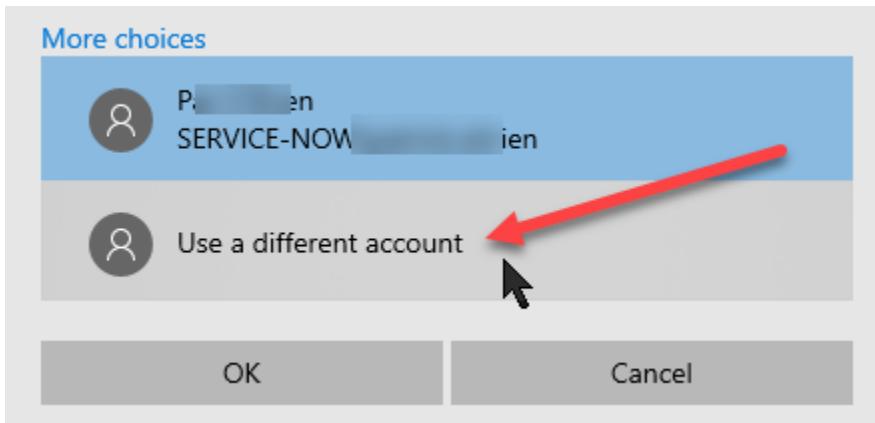
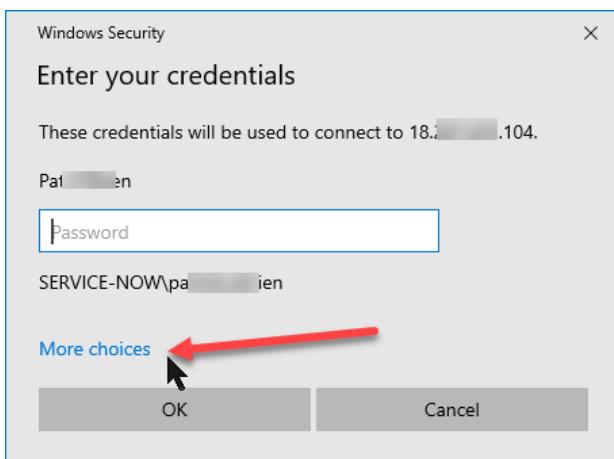
Note: This requires a remote desktop application. For Windows systems, use the built-in Remote Desktop Connection application. For MACs, use an application such as Microsoft Remote Desktop Connection.

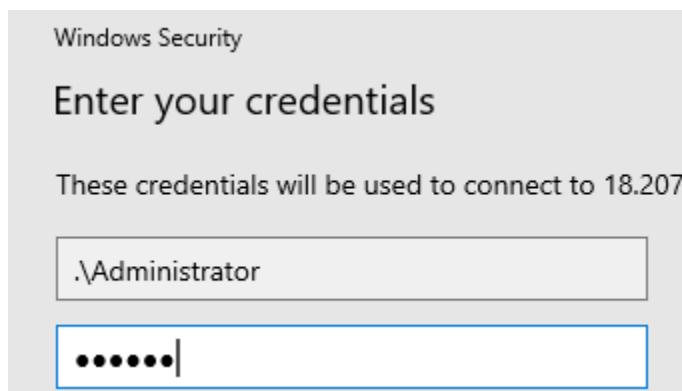


2. Log in via the remote desktop connection to the Windows server VM using the **MID SERVER RDP URL (FQDN)** and Administrator credentials from the Now Learning course page.

MID SERVER RDP URL nowlearning-nlinst00701720-mid-001.lab.service-now.com	MID SERVER PASSWORD LwLE[REDACTED]qzk (Username: Administrator)
INSTANCE STATUS Paused Terminate instance	Your instance will expire in... 2 Days 16 Hours 26 Minutes Request Expiry Extension
Open My Instance	
Wake Up Instance	

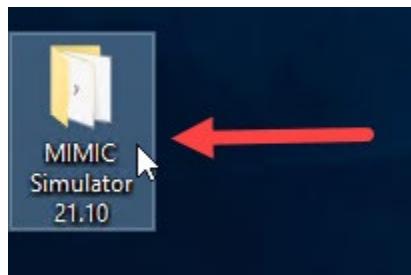
Note: Windows server public IP addresses will change after waking from hibernation.



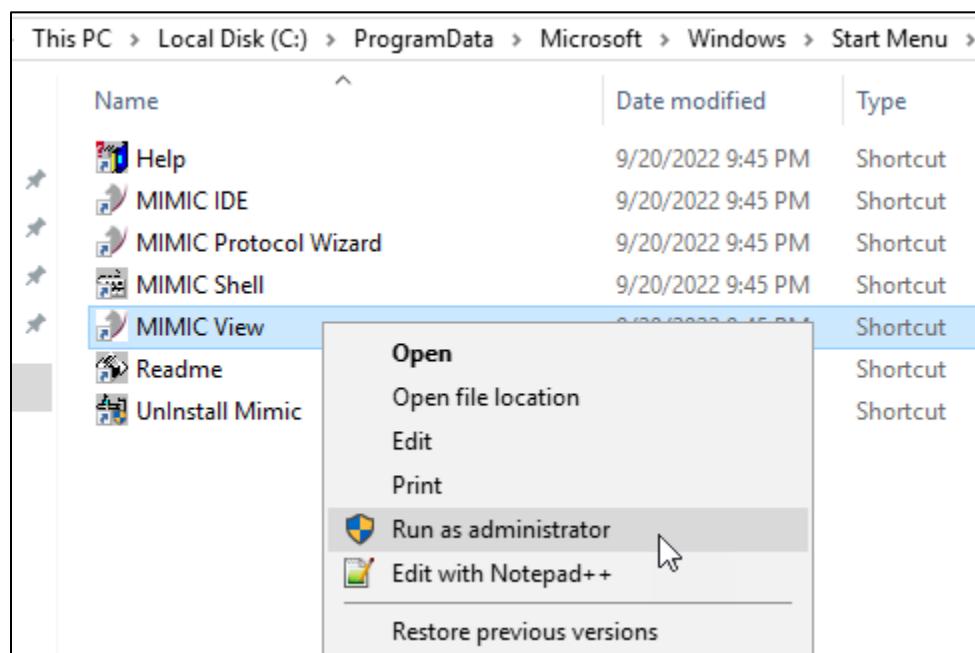


Note: Latest Windows security features prevent “pasting” of password into the RDP application if your session times out and locks. Our complex passwords will need to be typed in, so try to complete the lab without the remote desktop session locking.

3. On the Windows server desktop, open the **MIMIC Simulator** folder.

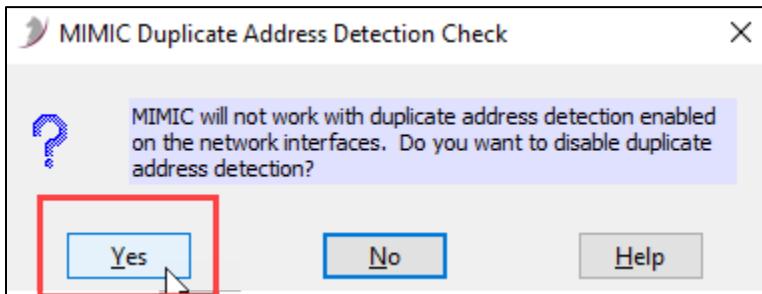


4. Right-click **MIMIC View** and click **Run as administrator**.

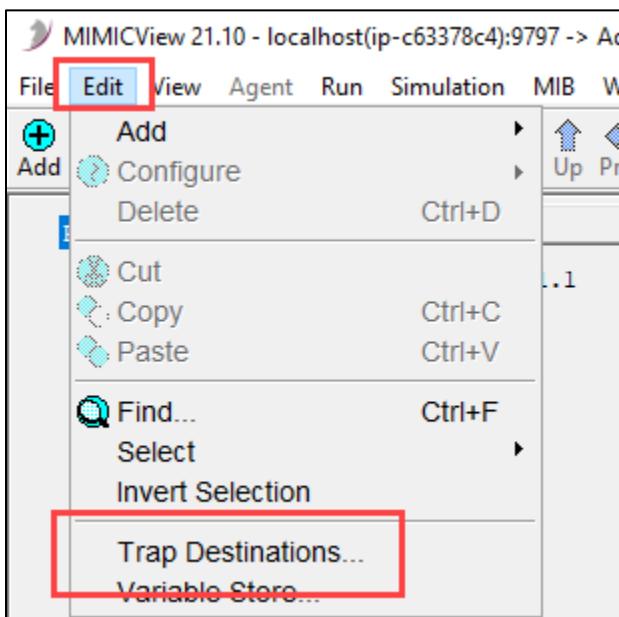


Note: *MIMIC View must be run as administrator.*

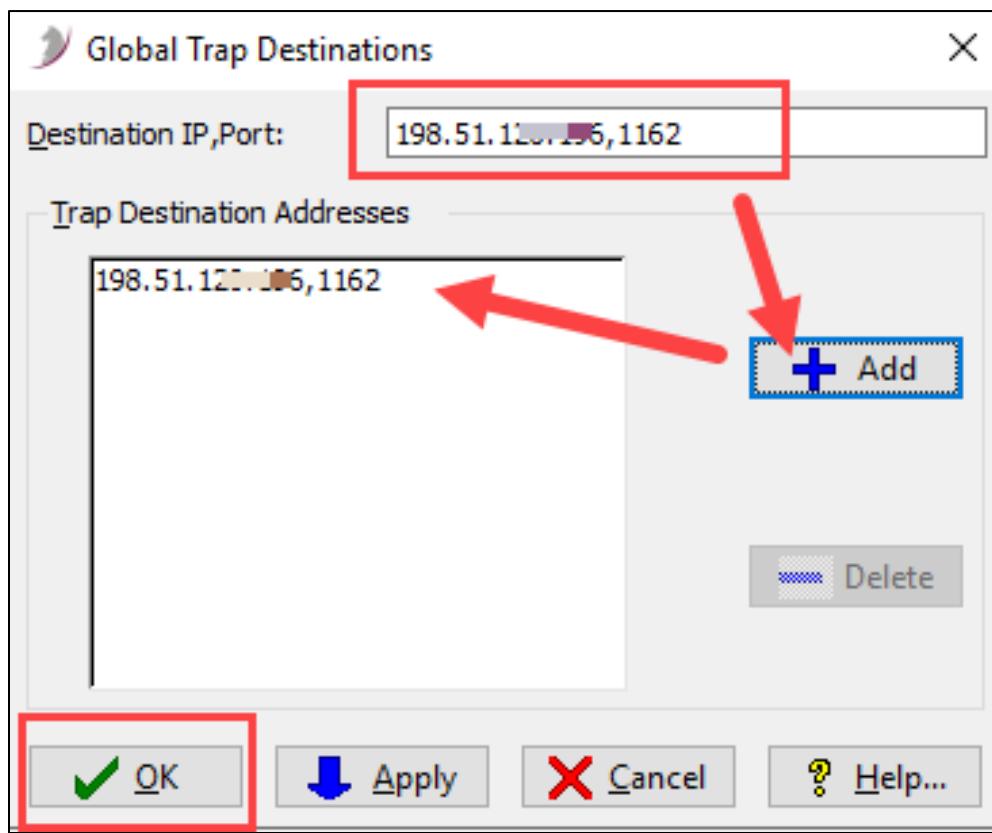
5. Click **Yes** at the User Account Control pop-up.
6. In the license pop-up, scroll to the bottom then click **OK**.
7. Click **Don't Notify** at the update software pop-up.
8. Click **Yes** at the duplicate address detection pop-up.



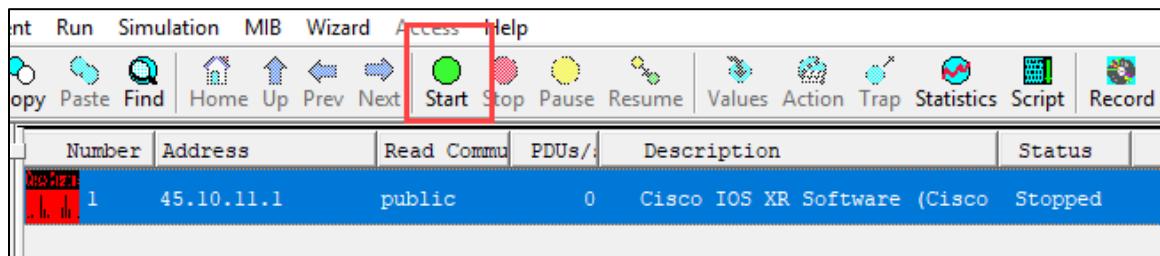
9. Click **OK** at the tutorial pop-up, then **Exit** the tutorial.
10. In MIMICView, click **Edit > Trap destinations**.



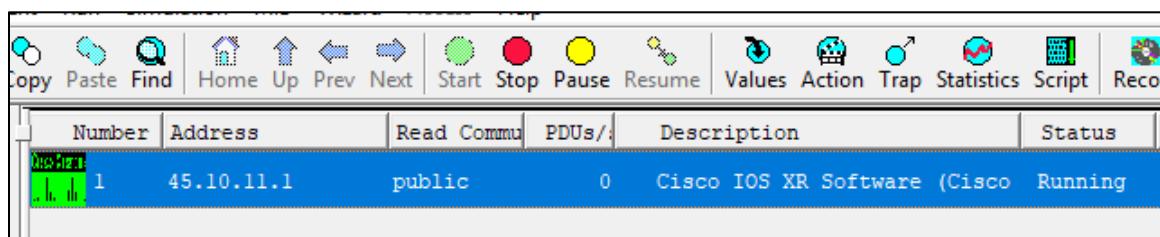
11. In the *Destination IP,Port* field, enter your MID Server's **private IP address** followed by **,1162**. Click **Add**, then **OK**. A comma separates the IP address from port number.



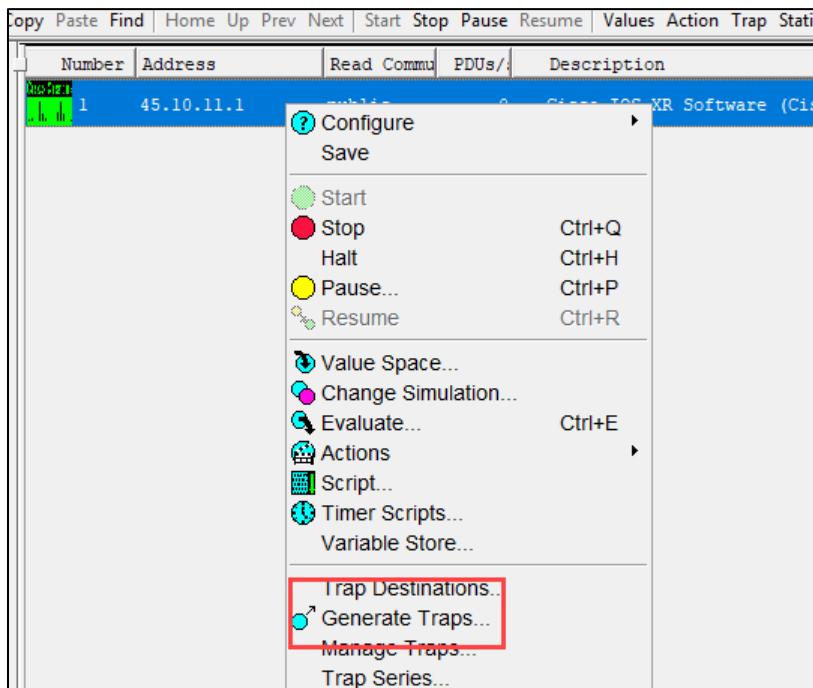
12. In the MIMIC menu bar, with the Cisco agent selected, click **Start**.



13. In a few seconds, the agent turns green and has a status Running.



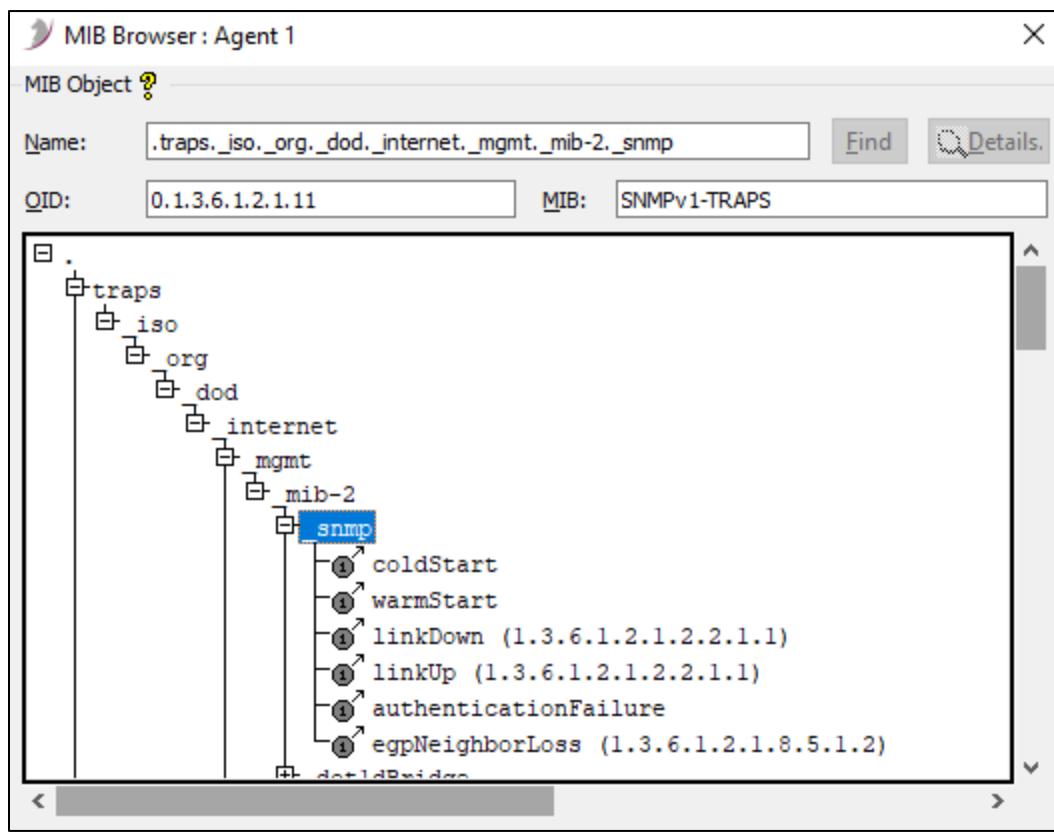
14. Right-click the Cisco agent and click **Generate Traps**.



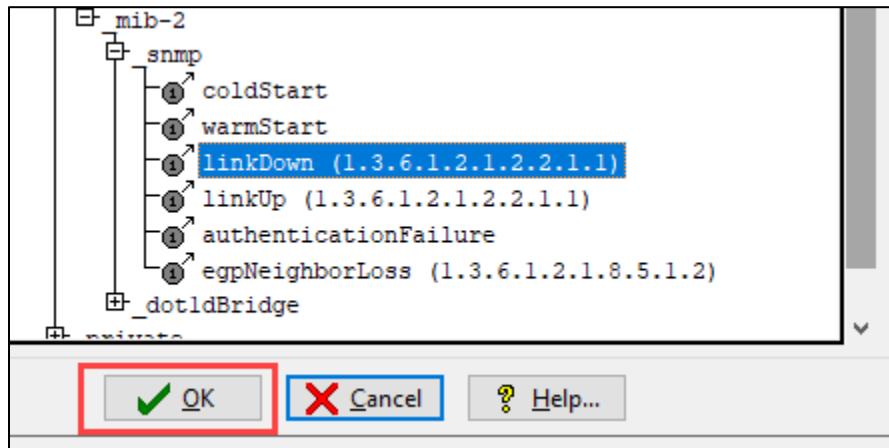
15. In the Generate Traps form General tab, click **Browse**.



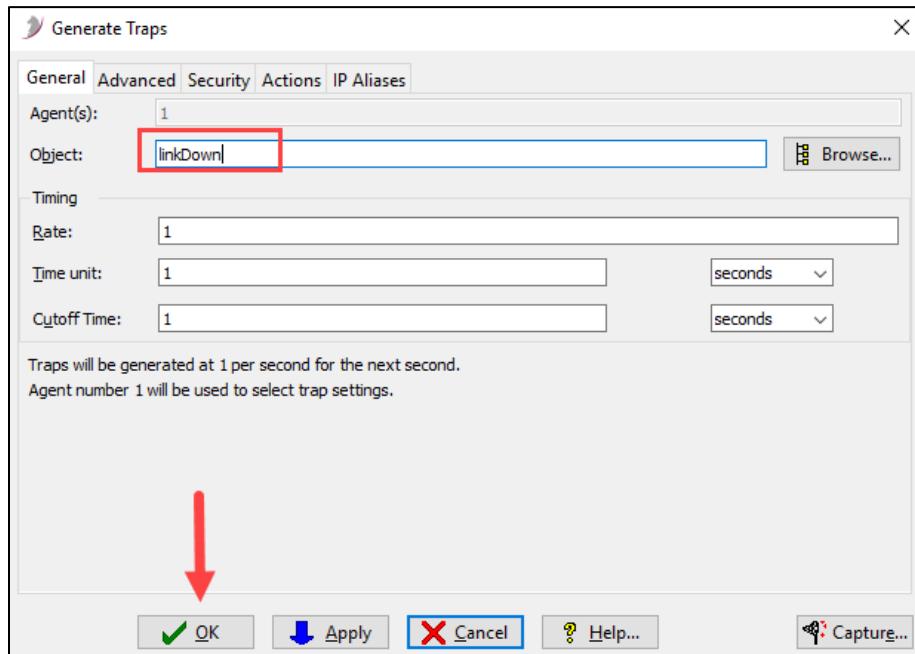
16. In the MIB Browser, drill down through traps > iso > org > dod > internet > mgmt > mib-2 > snmp to expose the traps.



17. Select the **linkDown** trap and click **OK**.



18. linkDown appears in the Object field. Click **OK**.



19. A single trap is generated.

20. Return to your ServiceNow instance and access **All Events**. Locate the event created by the trap with a source of **SNMPv1 Generic Trap**.

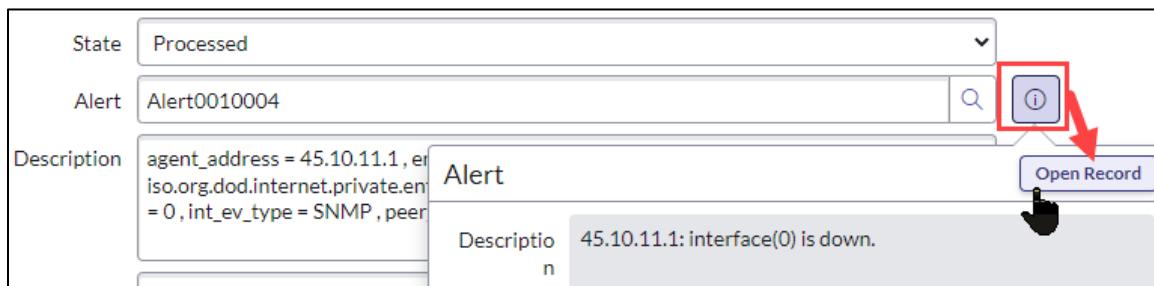
Events					
All > Created on Today					
	Time of event	Source	Description	Node	Type
	2023-03-01 22:33:31	SNMPv1 Generic Trap	agent_address = 45.10.11.1, enterprise ...		

21. Open the event. Note that there is no Node or Severity, yet an alert is created. [Read the Processing Notes](#).

Processing Notes	Binding alert CI process flow: Node is IP address Node was not found, checking by name Event CI type is empty No CI found for binding (Failed to resolve the event node to CI id) Binding Failure Reason: Failed to find the host with name: 45.10.11.1
Event rule applied: snmpV1.linkDown	

Note: ServiceNow Event Management includes many baseline SNMP event rules for processing SNMP traps.

22. Open the corresponding alert.

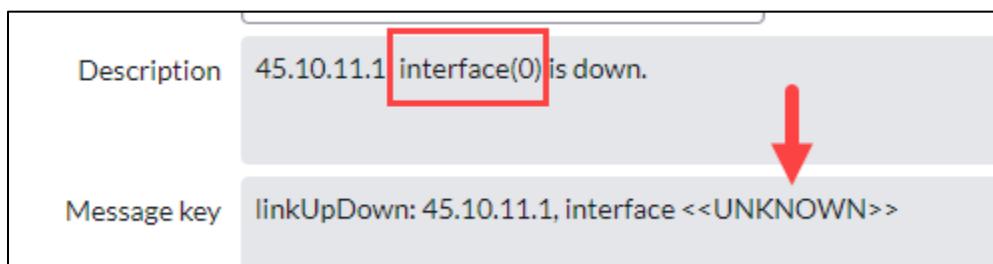


State	Processed
Alert	Alert0010004
Description	agent_address = 45.10.11.1, er iso.org.dod.internet.private.en = 0, int_ev_type = SNMP , peer

Alert

Description	45.10.11.1: interface(0) is down.
-------------	-----------------------------------

23. Note the severity is Warning, and that the Message key contains an error, interface <<UNKNOWN>>.



Description	45.10.11.1 interface(0) is down.
Message key	linkUpDown: 45.10.11.1, interface <<UNKNOWN>>

Note: We can deduce that there is an error in the event rule populating the message key, because we can see in the Description field that the interface = 0.

24. Navigate to **Event Management > Rules > Event Rules** and filter for **Name = *snmp**.

All > Name contains snmp					
<input type="checkbox"/>	Name ▲	Active	Order	Source	Apply addi
	*snmp	Search	Search	Search	Search
	snmpV1.authenticationFailure	true	100	SNMPv1 Generic Trap	false
	snmpV1.coldStart	true	100	SNMPv1 Generic Trap	false
	snmpV1.egpNeighborLoss	true	100	SNMPv1 Generic Trap	false
	snmpV1.linkDown	true	100	SNMPv1 Generic Trap	false
	snmpV1.linkUp	true	100	SNMPv1 Generic Trap	false

25. Open and review the **snmpV1.linkDown** event rule.

CHALLENGE 1

1. The trap indicates link down, yet the event rule (snmpV1.linkDown) populates a severity of Warning (4). Modify the event rule to set an alert severity of Major (2).
2. Fix the event rule (snmpV1.linkDown) so that the Message key correctly displays Interface (0), as is seen in the description field.
3. Modify the event rule (snmpV1.linkDown) by adding a threshold, such that 3 consecutive traps are required within a 10 second window before an alert is created. Test the threshold using the MIMIC Simulator.

Hint to send multiple traps (one per second for 5 seconds):

Generate Traps

General Advanced Security Actions IP Aliases

Agent(s): 1

Object: linkDown

Timing

Rate: 1

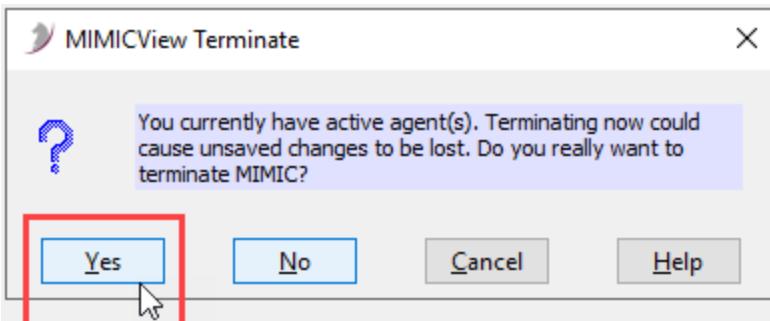
Time unit: 1 seconds

Cutoff Time: 5 seconds

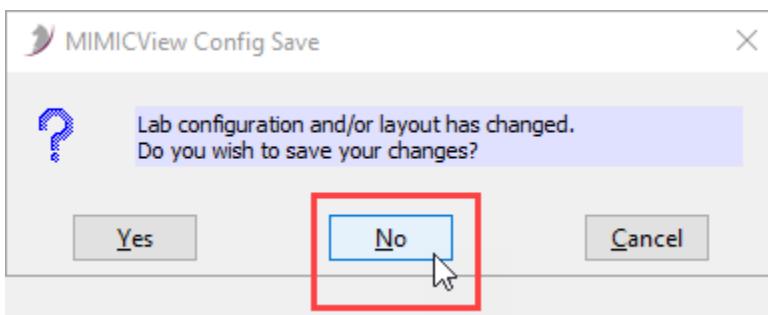
Traps will be generated at 1 per second for the next 5 seconds.
Agent number 1 will be used to select trap settings.

4. In MIMICView, click **File > Terminate**.

5. Click **Yes** to confirm termination.



6. Click **No** on the Config Save pop-up.



CHALLENGE 1 – Possible Solution

The screenshot shows the Event Rule configuration interface. The rule name is "Event Rule snmpV1.linkDown". The interface includes tabs for Event Rule Info, Event Filter, and Transform and Compose (selected). Below these tabs is a section titled "Transform and Compose Alert Output" with the sub-instruction: "Compose Alert fields by adding free text and by dragging variables from the right pane. Click Event Raw values to create new regex expressions." The "Severity" field is highlighted with a red box and contains the value "2". Other fields include Description, Node, Type, Resource, Message key, and Metric name.

Description	`\${node}: interface(\${ifIndex}) is down.
Node	`\${node}
Type	interface linkUpDown
Resource	interface \${ifIndex}
Message key	linkUpDown: \${node}, interface \${ifIndex}
Severity	2
Metric name	`\${metric_name}

Event Rule
snmpV1.linkDown

Event Rule Info Event Filter Transform and Compose Alert Output

Transform and Compose Alert Output

Compose Alert fields by adding free text and by dragging variables from the right pane.
Click Event Raw values to create new **regex expressions**.

Description	<code> \${node}: interface(\${ifIndex}) is down.</code>
Node	<code> \${node}</code>
Type	interface linkUpDown
Resource	interface \${ifIndex}
Message key	linkUpDown: \${node}, interface \${ifIndex}
Severity	4
Metric name	<code> \${metric_name}</code>

s/b ifIndex

Event Rule
snmpV1.linkDown

Event Rule Info Event Filter Transform and Compose Alert Output

Threshold

Select to create alerts only when the incoming matching events pass over the specified threshold. Once selected, other related values can be specified.

<input checked="" type="checkbox"/> Active	
Create Alert Operator	Count
* Occurs	3
* Over(seconds)	10
Close Alert Operator	Idle
* Over(seconds)	30

Congratulations on completing the lab!

Event Sources

Use Agent Client Collector Monitoring

Lab

5.4

45m

Lab Objectives

You will achieve the following objectives:

- Review the MID Server configuration for ACC Monitoring
- Activate ACC policies for monitoring
- Modify a check instance and republish a policy

Scenario

Agent Client Collector Monitoring (ACC-M) enables you to monitor your service availability, examine the health and performance of your environment, and ensure that your infrastructure and its applications are running properly. ACC is a ServiceNow provided event source.

MetricBase, the ServiceNow time series database required for processing metrics, is not enabled in the student instances. This will prevent metric data from displaying.

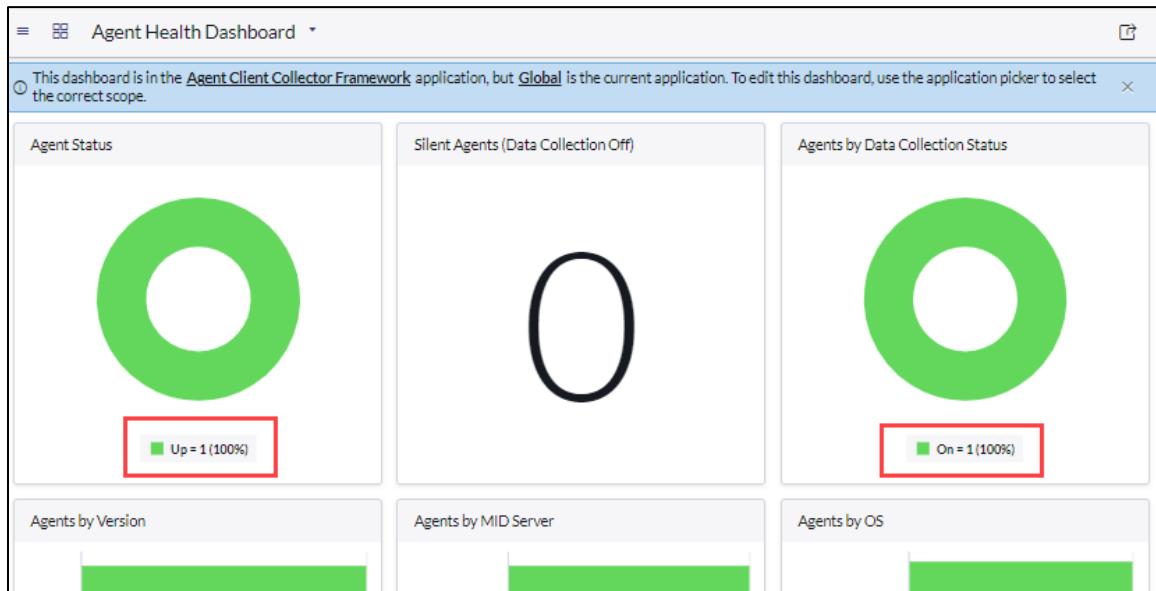
In this lab, you will activate Agent Client Collector policies and review the results.

Note: The Agent Client Collector Monitoring and Visibility store apps have already been installed on your ServiceNow instance. The ACC agent has also already been installed on your Windows MID Server, and the MID has been partially configured for ACC monitoring. Refer to the Agent Client Collector installation documentation for details or take the Agent Client Collector Essentials on-demand course found in ServiceNow's training site.

A. Verify agent installation and MID Server configuration for Agent Client Collector Monitoring

1. From your ServiceNow instance, navigate to **Agent Client Collector > Agent Health Dashboard**.

2. Ensure there is 1 agent Up and 1 agent on.



3. Navigate to **Agent Client Collector > Agents** to view the agent list.
4. The agent listed should have Host data collection = **Collected** and Configured Checks = **2**.

Name	Status	Host data collection	Host	Class	Mid	IP Address	Up since	Configured Checks	Data Coll
Agent_IP-C63385E1	Up	Collected	ip-c63385e1	Windows Server	windows_mid	198.51.133.225	2023-03-09 15:48:10	2	On

Note: With ACC-Visibility also installed, 2 checks (Enhanced Discovery and Installed Software) are enabled by default.

5. Click **windows_mid** to open the MID Server record.

Action	Host	Class	Mid	IP Address	Up since
	ip-198-51-65-29	Windows Server	windows_mid	198.51.65.29	2023-05-24 18:57:59

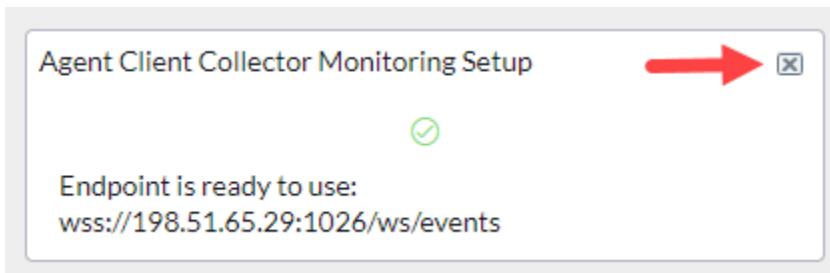
2. In the MID Server **Related Links**, click **Setup ACC Monitoring** to complete the MID configuration for ACC.

Related Links

[Rekey](#)
[Invalidate](#)
[Setup Metric Intelligence](#)
[Enable Credential-less Discovery](#)
[Grab Agent Client Collector Statistics](#)
[Grab MID logs, settings and thread dump](#)
[Lifecycle Events](#)
[Setup ACC Listener](#)
[Setup ACC Monitoring](#)
[Start JEP Recording](#)
[Trigger ACC certificate sync](#)
[Try redistributing connected agents](#)
[Create MID Profile](#)

Note: This related link also enables metrics collection (Metric Intelligence) since the plugin and required store apps are installed on your student instance. For more information see “Enable Metrics Collection and Evaluation” in the Agent Client Collector documentation.

3. Close the pop-up when the endpoint is ready.



4. Wait 60 seconds, then refresh the form.
5. To verify the configuration is correct, select the **Capabilities** related list.

6. Ensure that **Metrics**, **AgentClientCollector**, **Monitoring**, and **ALL** are present.

MID Server Issues	Configuration Parameters (6)	Supported Applications (2)	IP Ranges (1)	Capabilities (4)	Included in Clusters (1)
Extension Contexts (4)	Logs (39)	Threads (128)	Properties	Privileged Command	Applicative Credentials
Azure Service Principals	Data Sources	Discovery Functionality	Export Targets	HTTP Methods	SOAP Message Functions
MID server = windows_mid	Capability	Search		Actions on selected rows...	
	<input type="checkbox"/> Capability				
	Metrics			(empty)	
	Monitoring			(empty)	
	ALL			(empty)	
	AgentClientCollector			(empty)	

7. Open the **Extension Contexts** related list and ensure the three extensions are started.

MID Server Issues	Configuration Parameters (6)	Supported Applications (2)	IP Ranges (1)	Capabilities (4)	Included in Clusters (1)
Extension Contexts (4)	Logs (39)	Threads (128)	Properties	Privileged Command	Applicative Credentials
Azure Service Principals	Data Sources	Discovery Functionality	Export Targets	HTTP Methods	SOAP Message Functions
Executing on = windows_mid	Name	Search		Actions on selected rows...	
	<input type="checkbox"/> Name				
	mid_metrics_windows_mid	Operational Intelligence Metrics	Automatically created extension using th...	Started	
	mid_webserver_windows_mid	Mid Web Server	Automatically created extension using th...	Started	
	mid_websocket_windows_mid	ACC Websocket Endpoint	Automatically created extension using th...	Started	
	SNMP Trap Collector EM	TrapExtension		Started	

- Open the **Included in Clusters** related list and ensure there is one present.

MID Server Issues	Configuration Parameters (6)	Supported Applications (2)	IP Ranges (1)	Capabilities (4)	Included in Clusters (1)	
Extension Contexts (4)	Logs (39)	Threads (128)	Properties	Privileged Command	Applicative Credentials	Attachments
Azure Service Principals	Data Sources	Discovery Functionality	Export Targets	HTTP Methods	SOAP Message Functions	
<input type="button" value="≡"/> <input type="button" value="▼"/> <input type="button" value="MID server cluster"/> <input type="text" value="Search"/> <input type="button" value="Actions on selected rows..."/>						<input type="button" value="E"/>
MID server = windows_mid <input type="checkbox"/> <input type="button" value="Q"/> MID server cluster sn-acc-cluster-windows_mid						

B. Enable Windows policies

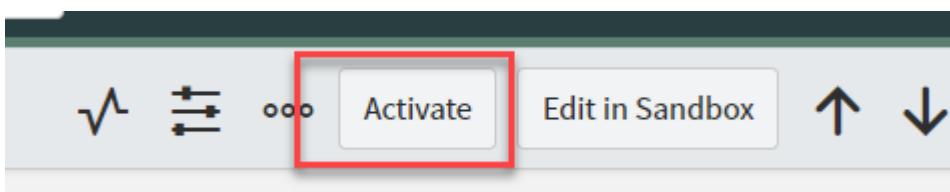
With an agent installed, we can activate applicable policies to monitor the server and applications running on it.

- Navigate to **Agent Client Collector > Configuration > Policies**.
- Locate the **Windows OS Events**, **Windows OS Metrics**, and **Windows Log monitoring** policies.

Name	Hierarchy	Active
Windows OS Metrics	None	false
Windows OS Events	None	false
Windows Log monitoring	None	false

Note: Do not enable Windows OS Events – Extended. Without MetricBase installed, metrics will not be captured or displayed.

- Open each policy separately, review the monitored CI's filter, review the check instances within the policy, and **activate** each policy with the UI action.



Name	Hierarchy	Active	Publ
Windows OS Metrics	None	true	Publ
Windows OS Events	None	true	Publ
Windows Log monitoring	None	true	Publ

4. Return to the **Agents** list and note the number of configured checks.

Install Status	Operational status	Configured Checks	Is duplicate	IP Add
Search	Search	Search	Search	Search
Installed	Operational	27	false	198.51

Note: The number of running checks may differ and take 1 to 2 minutes to display.

5. Navigate to **Event Management > All Events**. Note that the events include event checks and events to map metrics.

Time of event	Source	Description	Node	Type	Resource	Metric Name
2023-05-24 22:21:41	ITOM Agent	RAM Usage OK: The total memory utilization ...	IP-C633411D	os.windows.check-system-memory-percent		os.windows.metrics-system-memory-percent
2023-05-24 22:21:41	ITOM Agent	Windows Log CRITICAL: Found 2 criticals...	IP-C633411D	os.windows.check-log		os.windows.check-log
2023-05-24 22:21:36	ITOM Agent	CPU Load OK: The total CPU utilization ...	IP-C633411D	os.windows.check-system-cpu-load		os.windows.metrics-system-cpu-load
2023-05-24 22:21:23	ITOM Agent	Event to map a metric: ci_id:c0701889854...	IP-C633411D			disk.AvgDisksec/Write
2023-05-24 22:21:23	ITOM Agent	Event to map a metric: ci_id:c0701889854...	IP-C633411D			disk.DiskWriteBytes/sec
		Event to map a metric: ci_id:c0701889854...				

Note: The baseline "Windows Log monitoring" policy is meant to be modified before deploying into production, defining what log files the policy should monitor ("file" parameter). Without modification, it monitors the ACC log file for keywords ("pattern" parameter) and generates alerts in a **few minutes**, which is helpful in this lab.

The screenshot shows the 'Check Parameters' configuration screen. At the top, there are tabs for 'Check Parameters (4)', 'Check Secure Parameters', and 'Plugin (1)'. Below the tabs is a search bar with the placeholder 'for text' and a dropdown menu set to 'Search'. The main area is titled 'Check Parameters' and contains a table with two rows:

	Name	Value
<input type="checkbox"/>	warning	1 C:\ProgramData\ServiceNow\agent-client-collector\log\acc.log
<input type="checkbox"/>	critical	2
<input type="checkbox"/>	file	C:\ProgramData\ServiceNow\agent-client-c...
	pattern	"SEVERE Exception 404 Error"

6. Refresh the events list until these Windows Log events are shown, warning or critical. (Source = ITOM Agent)

The screenshot shows the 'Events' list. A tooltip on the left side of the screen displays the following log entry:

```
Windows Log CRITICAL: Found 2 criticals, 0 warnings for pattern  
SEVERE|Exception|404|Error in file  
C:\ProgramData\ServiceNow\agent-client-collector\log\acc.log . Warning Threshold: 1.  
Critical Threshold: 2
```

The event list table has columns: Type, Resource, Metric Name. There are three visible rows:

Type	Resource	Metric Name
os.windows.check-system-memory-percent		os.windows.metrics-system-memory-percent
ITOM Agent	Windows Log CRITICAL: Found 2 criticals...	os.windows.check-log
ITOM	CPU Load OK: The	

7. Open the corresponding alert then click Open in Workspace.

The screenshot shows an alert card for 'Alert - Alert001'. The card has a title bar with the alert name, a star icon, and a count of 6. Below the title are five buttons: 'Update', 'Go to Check Instance', 'Open in Workspace' (which is highlighted with a mouse cursor), 'Quick', and 'Details'. The main body of the card is mostly blank, with some very small text visible at the bottom right.

8. Review the Identified issue.

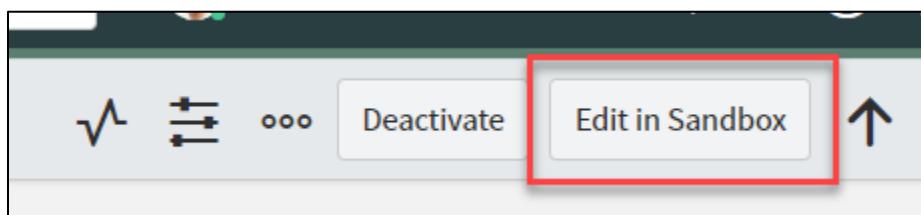
The screenshot shows a ServiceNow alert summary page. At the top, it displays the title "Windows Log WARNING: Found 0 criticals, 1 warnings for pattern SEVERE|Exception|...". Below this, there are several status indicators: Priority group (Low), Severity (Warning), State (Open), Initial event generation time (2024-06-12 18:43...), and Parent (Alert0010019). A navigation bar below these includes tabs for Overview, Details, Related records, Metrics, and Playbook. The "Overview" tab is selected. Under the "Summary" section, there is a box titled "Identified issue" containing a "Description" field. The description text is: "Windows Log WARNING: Found 0 criticals, 1 warnings for pattern SEVERE|Exception|404|Error in file C:\ProgramData\ServiceNow\agent-client-collector\log\acc.log . Warning Threshold: 1. Critical Threshold: 2".

C.Modify a Check Instance

Next, you will modify a check instance within a policy, causing a threshold to be breached and generate an alert.

The default Windows OS policy includes a memory usage check instance, which generates a warning alert if memory usage exceeds 85 % and a critical alert if usage exceeds 95%. To learn how to modify a check instance, you will change the “warn over” threshold to 5% to generate an alert.

1. Navigate to **Agent Client Collector > Policies** and open the **Windows OS Events** policy.
2. Click the **Edit in Sandbox** UI action.



3. In the **Check Instances** related list, locate and open the **os.windows.check-system-memory-percent**.

system-disk	true	Events	windows-disk -w {{.label...}}
os.windows.check-system-memory-percent	true	Events	winchecks check-windows-ram -w {{.labels...}}
os.windows.check-			winchecks check-

4. Note that the detailed description includes usage instructions. Scroll down to the Check **Parameters** related list and open **warning**.

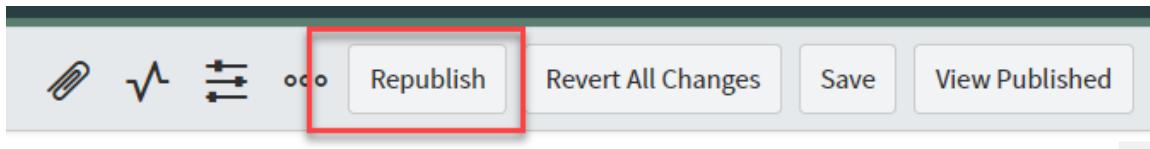
Check Parameters (2) Check Secure Parameters Plugin (1)						
New	Search for text	Search				
Check = os.windows.check-system-memory						
Check Parameters	Name	Value	Active	Mandatory	Flag	
<input type="checkbox"/>	warning	85	true	true	-w	
<input type="checkbox"/>	critical	95	true	true	-c	

5. Change the **-w** parameter **value** to **5**.

Name	warning
Active	<input checked="" type="checkbox"/>
Value	5 
Flag	-w
Check	os.windows.check-system-memory

6. On the Check Parameter form, click **Update**.
7. On the Check Instance form, click **Update**.

8. On the Policy form, click **Republish**.



9. On the confirmation pop-up, click **Publish**. The updated policy will be propagated out to the agents, which will implement the new check. This process can take several minutes.

10. To monitor the update being propagated to the agent, navigate to **Agent Client Collector > Agents**.

11. Click to open your agent record.

Name	Status	Host data collection	Host
Agent IP-C633411D	Up	Collected	ip-198-51-6

12. In Related Links, click **Recent Input ECC Queues**.

Related Links
Restart agent
Pause data collection
Clear Assets
Grab agent config.(acc.yml)
Grab agent log
Recent Input ECC Queues
Set Log Level
Show distribution of this proxyagent Cls
Subscribe
Test check
Upgrade agent

13. Sort the list by **Processed** column.

Created	Agent	Topic	Queue	State	Processed
2023-05-24 19:37:31	mid.server.windows_mid	MonitoringProbe	request	input	processed 2023-05-24 19:37:33
2023-05-24 18:59:25	mid.server.windows_mid	MonitoringProbe	request	input	processed 2023-05-24 18:59:32
2023-05-24 18:58:53	mid.server.windows_mid	MonitoringProbe	request	output	processed 2023-05-24 18:58:54

Note: These ECC queue records can be used for troubleshooting but are populated after the actual transaction takes place through the queue. These steps are for awareness of the queue records.

14. Within a few minutes, the policy will be implemented by the ACC, the 5% threshold will be exceeded, and an event generated. Navigate to **All Events**. Locate and open the system memory check.

Time of event	Type	Resource
2021-08-31 16:19:08	ITOM Agent	RAM Usage WARNING: The total memory uti...

15. The event will have generated an alert.

Message key	ed18ae28f8dab0107f444556b44331e9_#_ip-C633DE76_#_os.windows.check-system-memory-percent_#_e2a3268cc7250010b9a4362c14c26080
Severity	Warning
Resolution state	New
Time of event	2021-08-31 16:19:08
State	Processed
Alert	Alert0010092
Description	RAM Usage WARNING: The total memory utilization is 55.83% . Warning Threshold: 5. Critical Threshold: 95
Additional information	{"check_interval": "60", "reporting_mid": "windows_mid", "policy_name": "Windows OS Events", "check_name": "os.windows.check-system-memory-percent"}

16. From the event record, open the alert.

Alert

Source	ITOM Agent
Node	ip-C6337426
Type	os.windows.ch
Resource	
Metric Name	os.windows.m
source instance	
Message key	b601a25955a1:memory_#_e2:
Severity	Warning
resolution state	New
Time of event	2021-01-06 23:59:59
State	Processed
Alert	Alert0010021
Description	RAM Usage WARNING: The total memory utilization is 39.05% . Warning Threshold: 5. Critical Threshold: 95

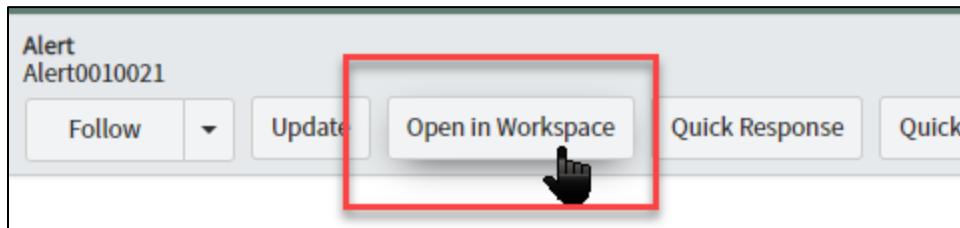
Open Record

Correlated Alerts

1

2

17. Click **Open in Workspace**.



18. Review the details of the alert in Service Operations Workspace.

Note: You have modified a check instance within a policy and published it to ACC. The very low threshold was quickly breached by the server, and an event generated by ACC. Event processing generated an alert. This completes the lab.

19. **Challenge:** Reverse the warn over change and republish the original policy.
Subsequent OK/Clear events should close the alert.

Congratulations on completing the lab and the course!

www.servicenow.com/services/training-and-certification.html



2225 Lawson Ln, Santa Clara, CA 95054, USA • (858) 720-0477 • (858) 720-0479 • www.servicenow.com

©2024 ServiceNow, Inc. All rights reserved.

ServiceNow believes information in this publication is accurate as of its publication date. This publication could include technical inaccuracies or typographical errors. The information is subject to change without notice. Changes are periodically added to the information herein; these changes will be incorporated in new editions of the publication. ServiceNow may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time. Reproduction of this publication without prior written permission is forbidden. The information in this publication is provided "as is". ServiceNow makes no representations or warranties of any kind, with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

ServiceNow is a trademark of ServiceNow, Inc. All other brands, products, service names, trademarks or registered trademarks are used to identify the products or services of their respective owners.