Reduce event noise with Event Compression in Enterprise Manager

Desiree Abrokwa
Product Management

Introduction

Desiree Abrokwa

Product Manager

Enterprise Manager (EM) 13.5

Hybrid Cloud Management

Fleet monitoring, management and data movement across entire IT estate – on-premises and in the cloud

Ops Automation

Enhanced automation and modernization of key management tasks

Extensibility

Open standards-based extensions for interoperability with 3rd party ecosystems

Background

- IT teams are often overwhelmed with volume of events
  - Many events are symptoms of the same underlying problem
- Event Compression is the process of grouping related events into a smaller subset of incidents
  - Helps reduce event noise
- First introduced *Rule-Based Event Compression*
- In EM 13.5, Event Compression enhancement: *Event Compression Policies*

Use Event Compression to reduce event noise

- Event Compression
- User-Defined Event Compression Policies
- Event Compression Analysis

Use Event Compression to reduce event noise

- Event Compression
- User-Defined Event Compression Policies
- Event Compression Analysis

Event Compression

Rule-Based Event Compression

- Specific to individual rule
- Define an event compression policy directly within a rule
- To create the same policy for another rule, you had to redefine it within the other rule definition

Event Compression Policies

- Apply to all incident creating rules
- Only have to define the policy once in the Event Compression Policies page
- Once enabled and an incident is created, EM will match the corresponding global policy to the incident that is in the process of creation

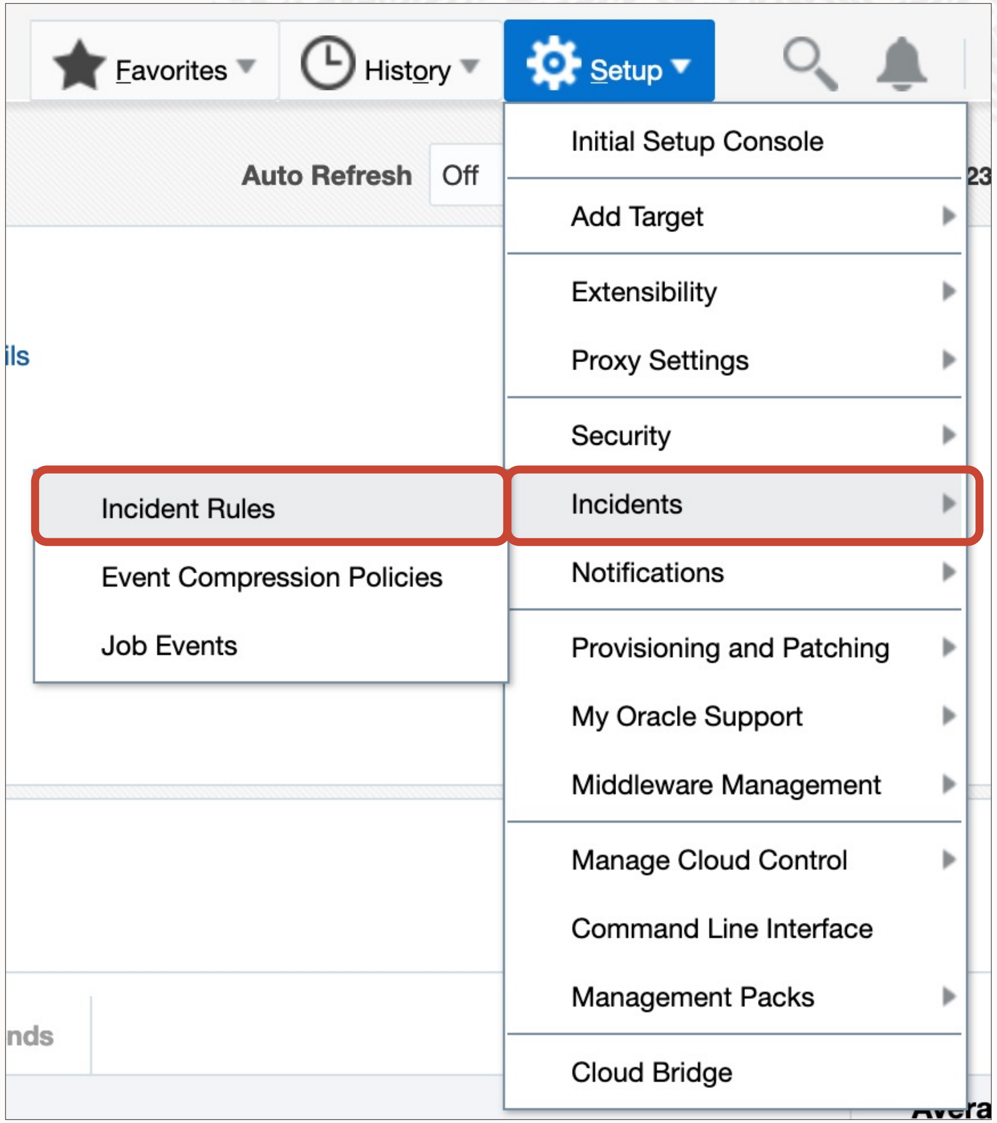
Rule-Based Event Compression

- Original method of Event Compression
- Compression completed in individual rules
- Implemented in two steps:
  - Create an event rule that compresses related events into a single incident
  - Create an incident rule to send a notification (email, ticket creation, etc.) when an incident is created
- Out-of-box incident rules that automatically group (compress) related events into single incidents
  - For example:
    - Target down for RAC database instances
    - Metric collection errors for a target
    - Configuration standard violations for a rule on a target

Rule-Based Event Compression

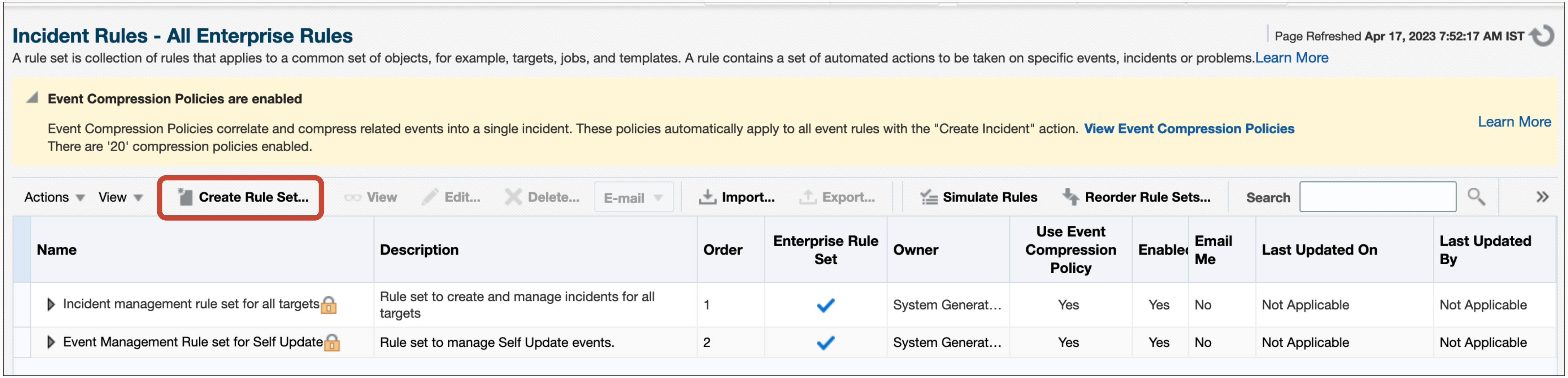
Navigating to Incident Rules

Setup > Incident > Incident Rules



Rule-Based Event Compression

Incident Rules - Create Rule Set



Incident Rules - All Enterprise Rules

Page Refreshed **Apr 17, 2023 7:52:17 AM IST**

A rule set is collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems.Learn More

Event Compression Policies are enabled

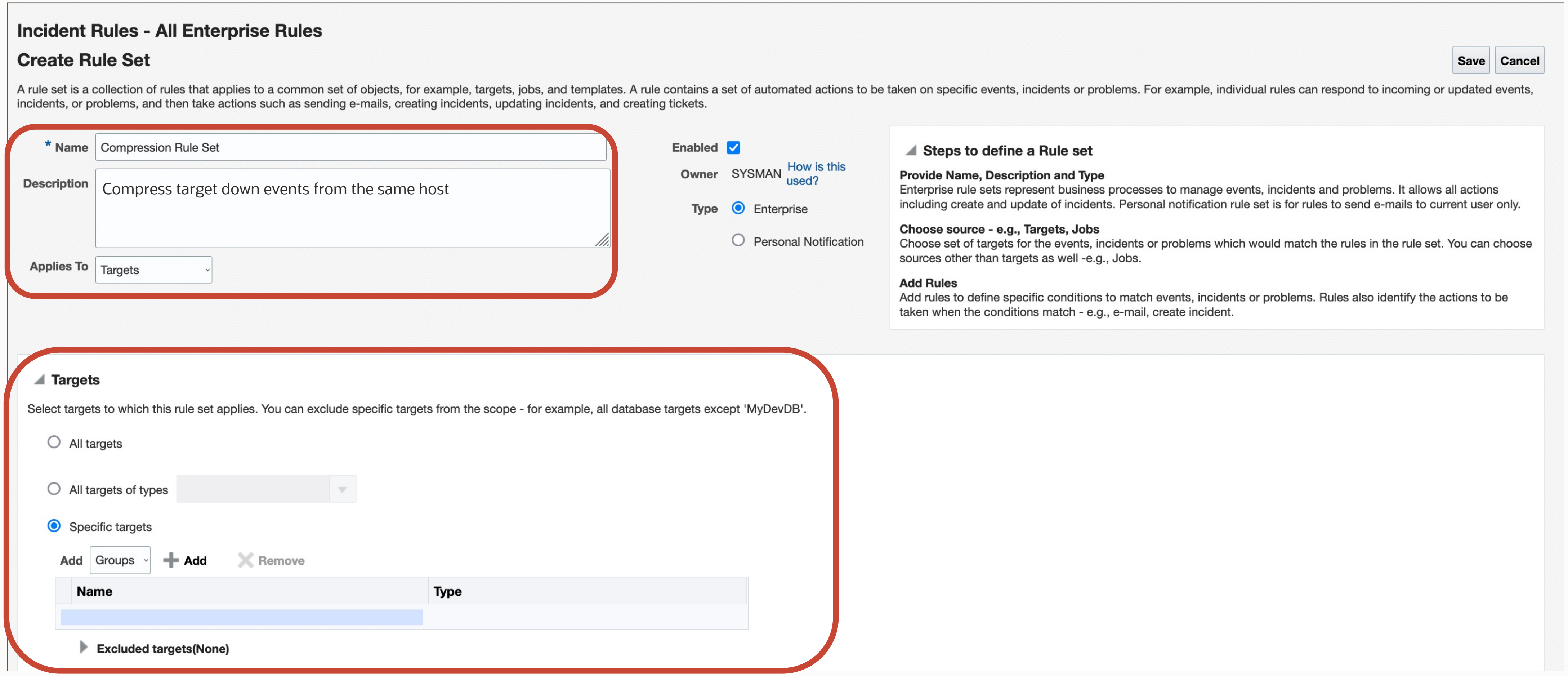
Event Compression Policies correlate and compress related events into a single incident. These policies automatically apply to all event rules with the "Create Incident" action. **View Event Compression Policies**
There are '20' compression policies enabled.

Learn More

Name	Description	Order	Enterprise Rule Set	Owner	Use Event Compression Policy	Enablec	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat...	Yes	Yes	No	Not Applicable	Not Applicable
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat...	Yes	Yes	No	Not Applicable	Not Applicable

Rule-Based Event Compression

Incident Rules - Specify the name of rule set and select targets to apply on



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name	Compression Rule Set
Description	Compress target down events from the same host
Applies To	Targets
Enabled	☑
Owner	SYSMAN How is this used?
Type	● Enterprise ○ Personal Notification

Steps to define a Rule set

Provide Name, Description and Type
Enterprise rule sets represent business processes to manage events, incidents and problems. It allows all actions including create and update of incidents. Personal notification rule set is for rules to send e-mails to current user only.

Choose source - e.g., Targets, Jobs
Choose set of targets for the events, incidents or problems which would match the rules in the rule set. You can choose sources other than targets as well -e.g., Jobs.

Add Rules
Add rules to define specific conditions to match events, incidents or problems. Rules also identify the actions to be taken when the conditions match - e.g., e-mail, create incident.

Targets

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except 'MyDevDB'.

○ All targets

○ All targets of types

● Specific targets

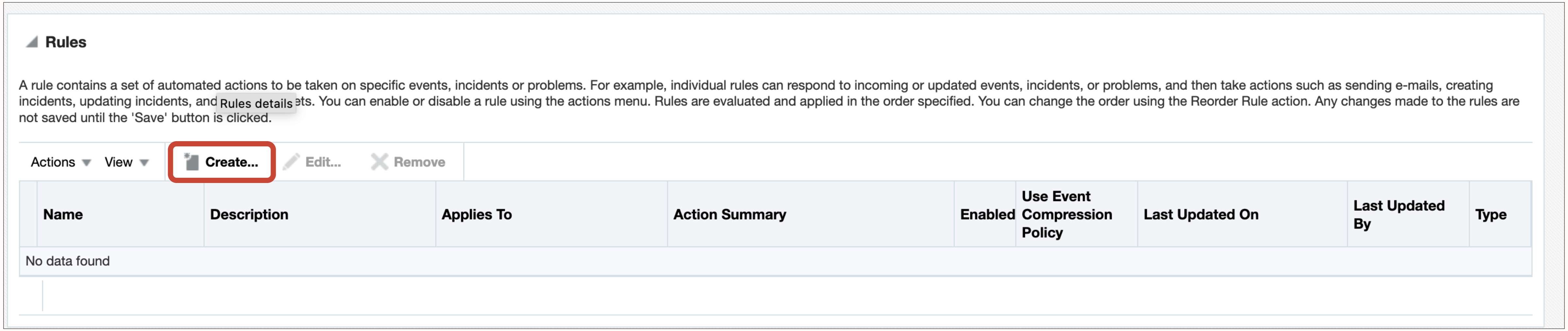
Add Groups ✚ Add ✕ Remove

Name	Type

▸ **Excluded targets(None)**

Rule-Based Event Compression

Incident Rules – Create rule



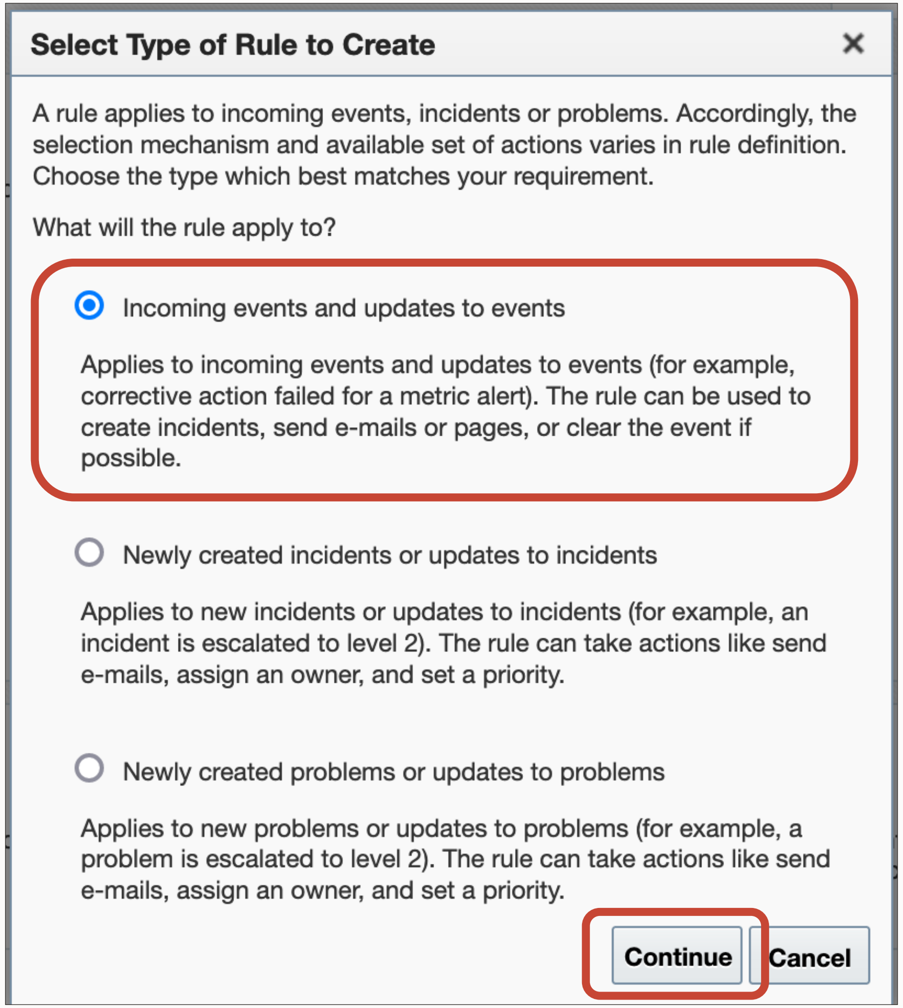
Rules

A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and Rules details ets. You can enable or disable a rule using the actions menu. Rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule action. Any changes made to the rules are not saved until the 'Save' button is clicked.

Name	Description	Applies To	Action Summary	Enabled	Use Event Compression Policy	Last Updated On	Last Updated By	Type
No data found								

Rule-Based Event Compression

Incident Rules – Select for incoming events



Select Type of Rule to Create

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

What will the rule apply to?

● Incoming events and updates to events

Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

○ Newly created incidents or updates to incidents

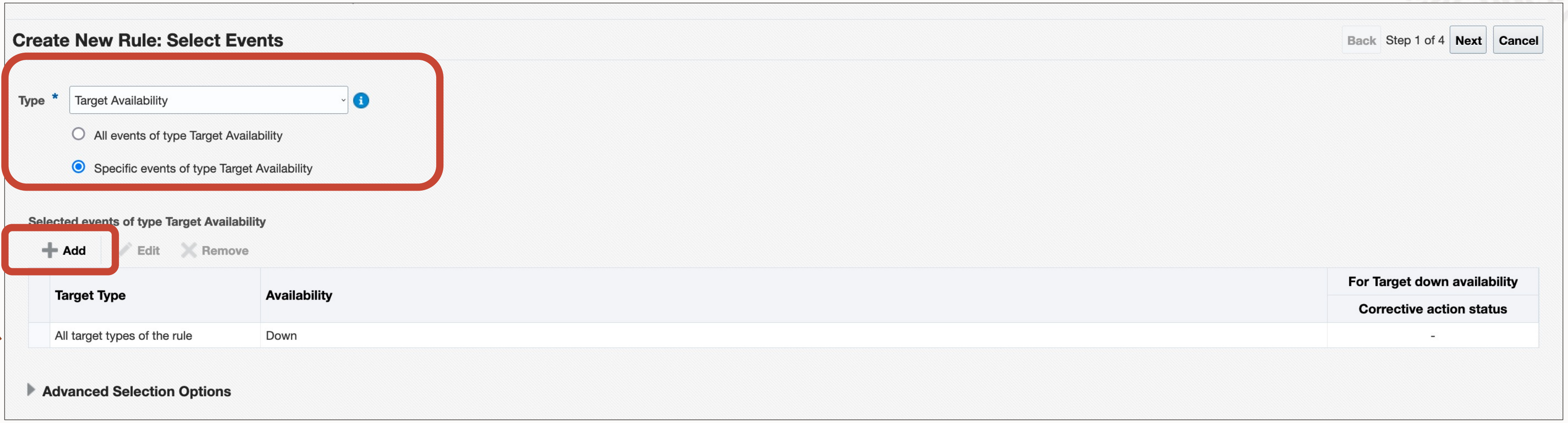
Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

○ Newly created problems or updates to problems

Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

Rule-Based Event Compression

Incident Rules - Select event types



Create New Rule: Select Events

Type * Target Availability

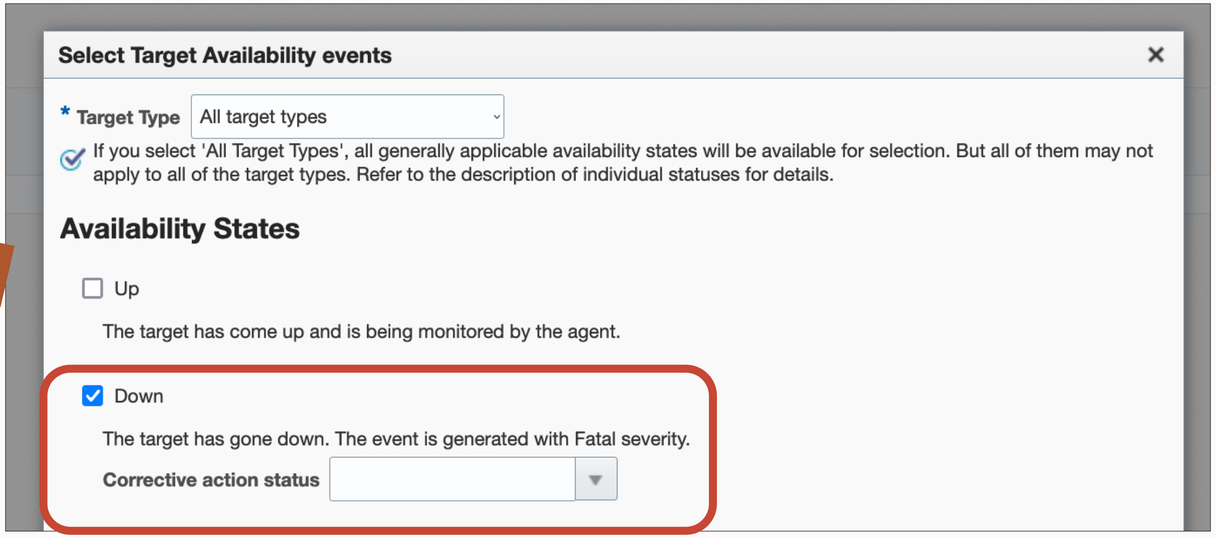
○ All events of type Target Availability

● Specific events of type Target Availability

Selected events of type Target Availability

Target Type	Availability	For Target down availability Corrective action status
All target types of the rule	Down	-

▸ Advanced Selection Options



Select Target Availability events

* Target Type: All target types

If you select 'All Target Types', all generally applicable availability states will be available for selection. But all of them may not apply to all of the target types. Refer to the description of individual statuses for details.

Availability States

☐ Up

The target has come up and is being monitored by the agent.

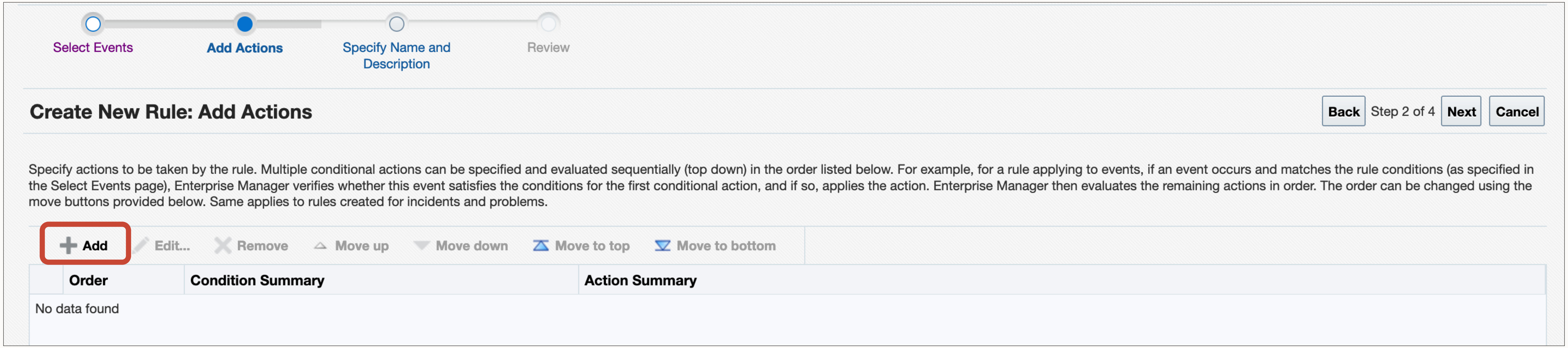
☑ Down

The target has gone down. The event is generated with Fatal severity.

Corrective action status

Rule-Based Event Compression

Incident Rules - Add actions



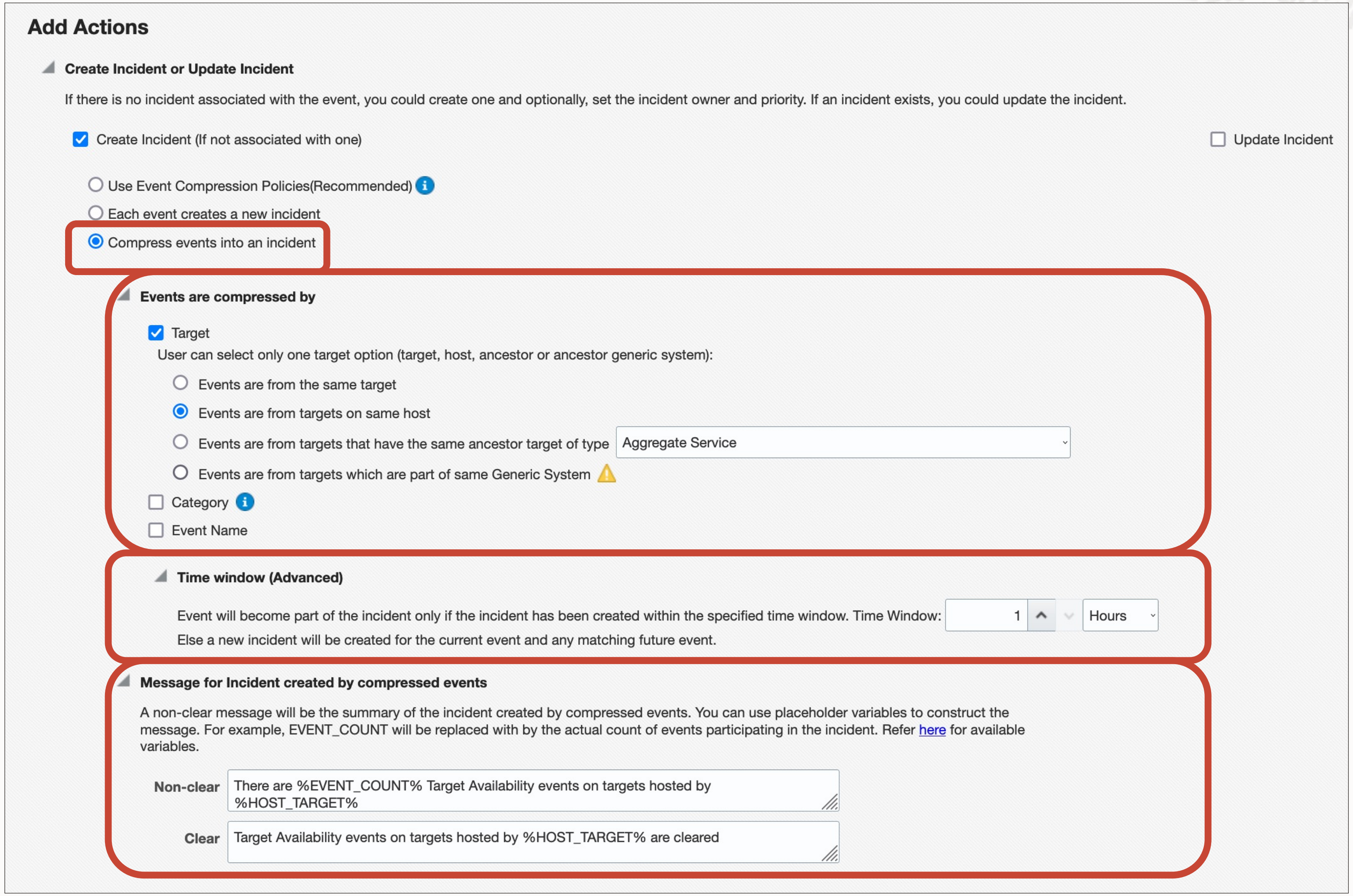
Create New Rule: Add Actions

Specify actions to be taken by the rule. Multiple conditional actions can be specified and evaluated sequentially (top down) in the order listed below. For example, for a rule applying to events, if an event occurs and matches the rule conditions (as specified in the Select Events page), Enterprise Manager verifies whether this event satisfies the conditions for the first conditional action, and if so, applies the action. Enterprise Manager then evaluates the remaining actions in order. The order can be changed using the move buttons provided below. Same applies to rules created for incidents and problems.

Order	Condition Summary	Action Summary
No data found		

Rule-Based Event Compression

Incident Rules – Add Actions



Add Actions

Create Incident or Update Incident

If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

☑ Create Incident (If not associated with one)

☐ Update Incident

○ Use Event Compression Policies(Recommended)

○ Each event creates a new incident

● Compress events into an incident

Events are compressed by

☑ Target

User can select only one target option (target, host, ancestor or ancestor generic system):

○ Events are from the same target

● Events are from targets on same host

○ Events are from targets that have the same ancestor target of type: Aggregate Service

○ Events are from targets which are part of same Generic System ⚠

☐ Category

☐ Event Name

Time window (Advanced)

Event will become part of the incident only if the incident has been created within the specified time window. Time Window: 1 Hours

Else a new incident will be created for the current event and any matching future event.

Message for Incident created by compressed events

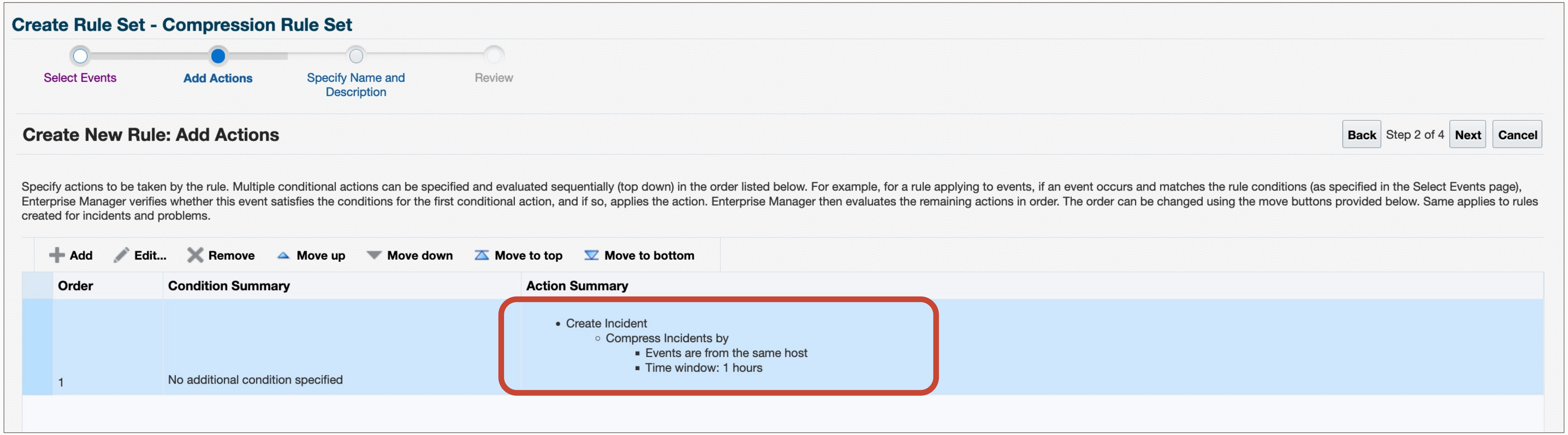
A non-clear message will be the summary of the incident created by compressed events. You can use placeholder variables to construct the message. For example, EVENT_COUNT will be replaced with by the actual count of events participating in the incident. Refer here for available variables.

Non-clear: There are %EVENT_COUNT% Target Availability events on targets hosted by %HOST_TARGET%

Clear: Target Availability events on targets hosted by %HOST_TARGET% are cleared

Rule-Based Event Compression

Incident Rules – Add Actions saved



Create Rule Set - Compression Rule Set

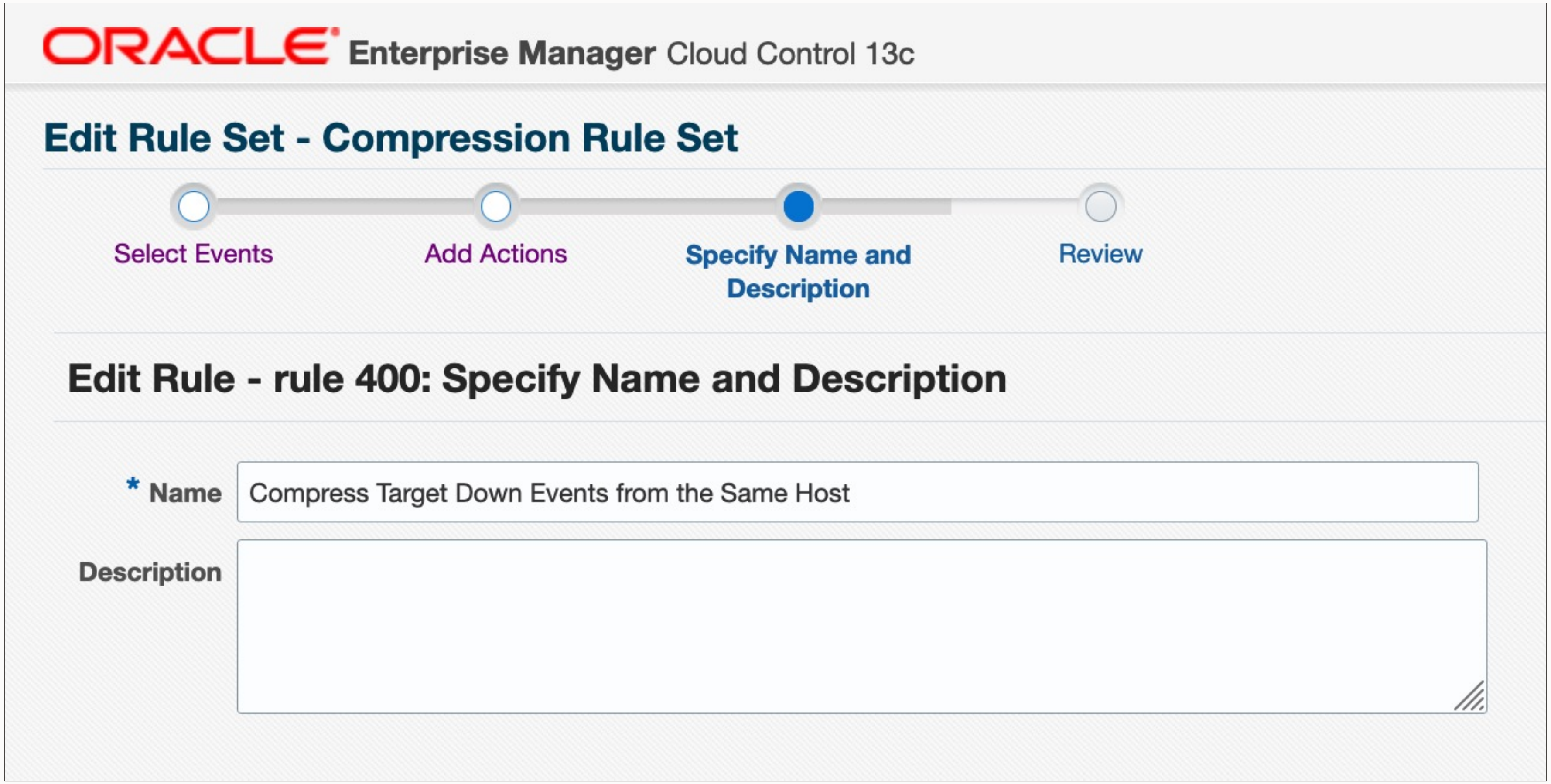
Create New Rule: Add Actions

Specify actions to be taken by the rule. Multiple conditional actions can be specified and evaluated sequentially (top down) in the order listed below. For example, for a rule applying to events, if an event occurs and matches the rule conditions (as specified in the Select Events page), Enterprise Manager verifies whether this event satisfies the conditions for the first conditional action, and if so, applies the action. Enterprise Manager then evaluates the remaining actions in order. The order can be changed using the move buttons provided below. Same applies to rules created for incidents and problems.

Order	Condition Summary	Action Summary
1	No additional condition specified	• Create Incident ◦ Compress Incidents by ▪ Events are from the same host ▪ Time window: 1 hours

Rule-Based Event Compression

Incident Rules – Specify name and description



ORACLE Enterprise Manager Cloud Control 13c

Edit Rule Set - Compression Rule Set

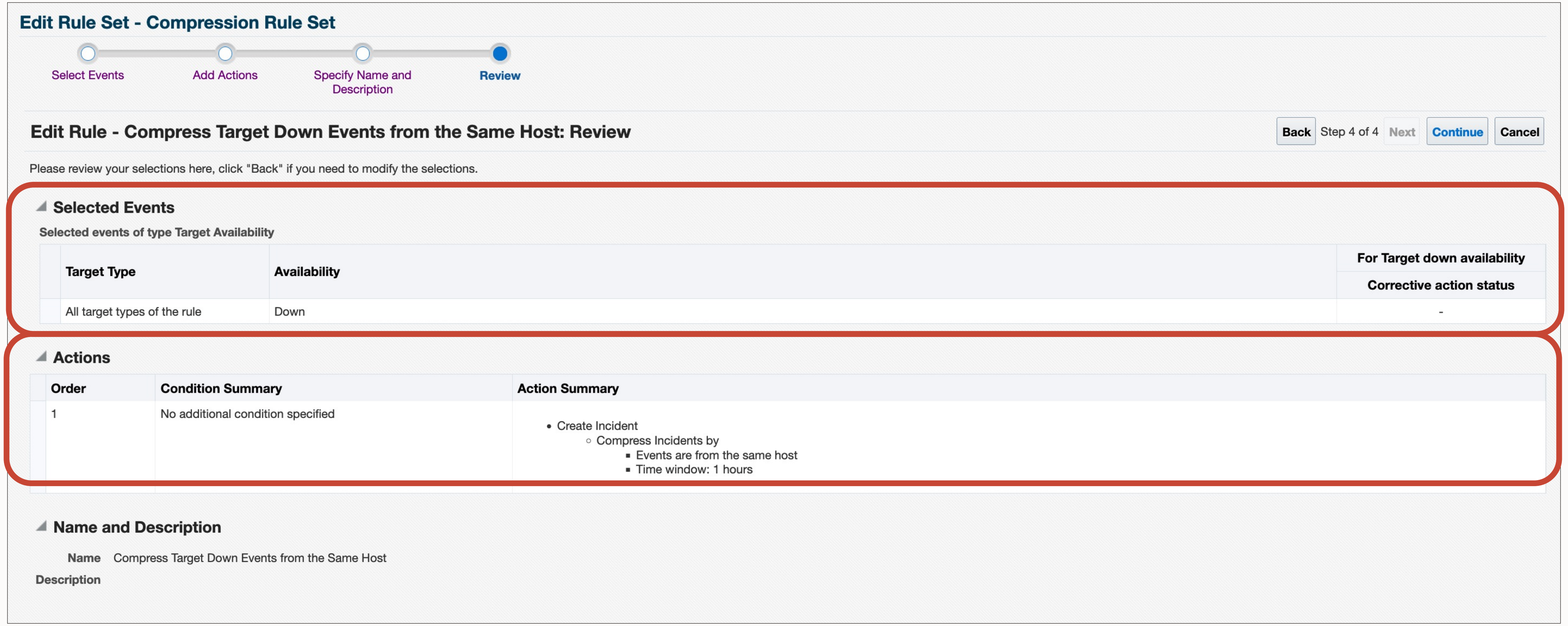
Edit Rule - rule 400: Specify Name and Description

* Name: Compress Target Down Events from the Same Host

Description:

Rule-Based Event Compression

Incident Rules – Review Rule Set



Edit Rule Set - Compression Rule Set
Select Events
Add Actions
Specify Name and Description
Review
Back
Step 4 of 4
Next
Continue
Cancel

Edit Rule - Compress Target Down Events from the Same Host: Review

Please review your selections here, click "Back" if you need to modify the selections.

Selected Events

Selected events of type Target Availability

Target Type	Availability	For Target down availability Corrective action status
All target types of the rule	Down	-

Actions

Order	Condition Summary	Action Summary
1	No additional condition specified	• Create Incident ○ Compress Incidents by ▪ Events are from the same host ▪ Time window: 1 hours

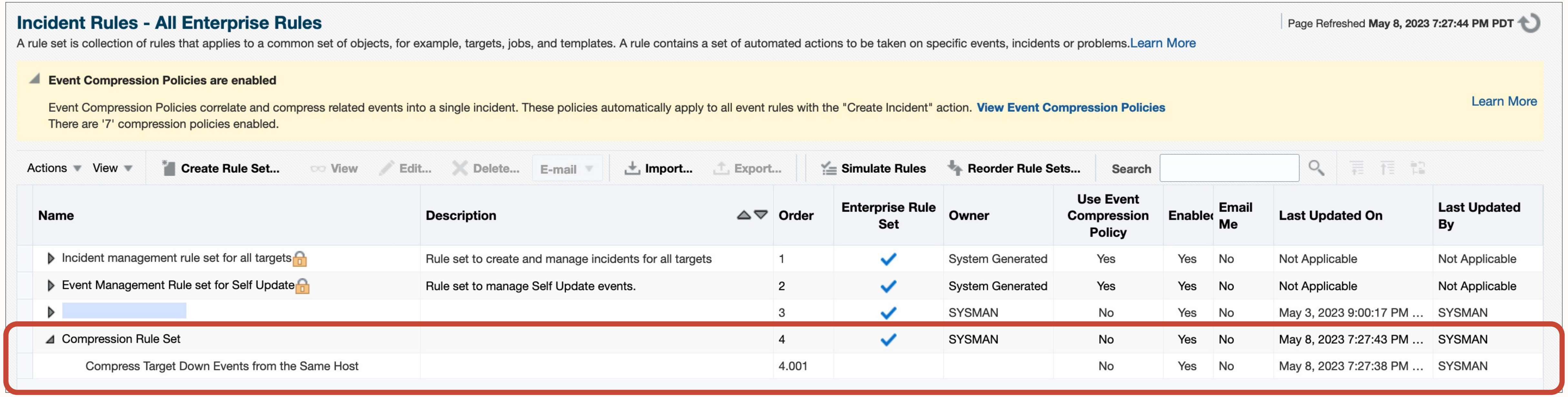
Name and Description

Name Compress Target Down Events from the Same Host

Description

Rule-Based Event Compression

Incident Rule created



Incident Rules - All Enterprise Rules

Page Refreshed **May 8, 2023 7:27:44 PM PDT**

A rule set is collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems.Learn More

Event Compression Policies are enabled

Event Compression Policies correlate and compress related events into a single incident. These policies automatically apply to all event rules with the "Create Incident" action. **View Event Compression Policies**
There are '7' compression policies enabled.

Learn More

Name	Description	Order	Enterprise Rule Set	Owner	Use Event Compression Policy	Enabled	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generated	Yes	Yes	No	Not Applicable	Not Applicable
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generated	Yes	Yes	No	Not Applicable	Not Applicable
[redacted]		3	✓	SYSMAN	No	Yes	No	May 3, 2023 9:00:17 PM ...	SYSMAN
Compression Rule Set		4	✓	SYSMAN	No	Yes	No	May 8, 2023 7:27:43 PM ...	SYSMAN
Compress Target Down Events from the Same Host		4.001			No	Yes	No	May 8, 2023 7:27:38 PM ...	SYSMAN

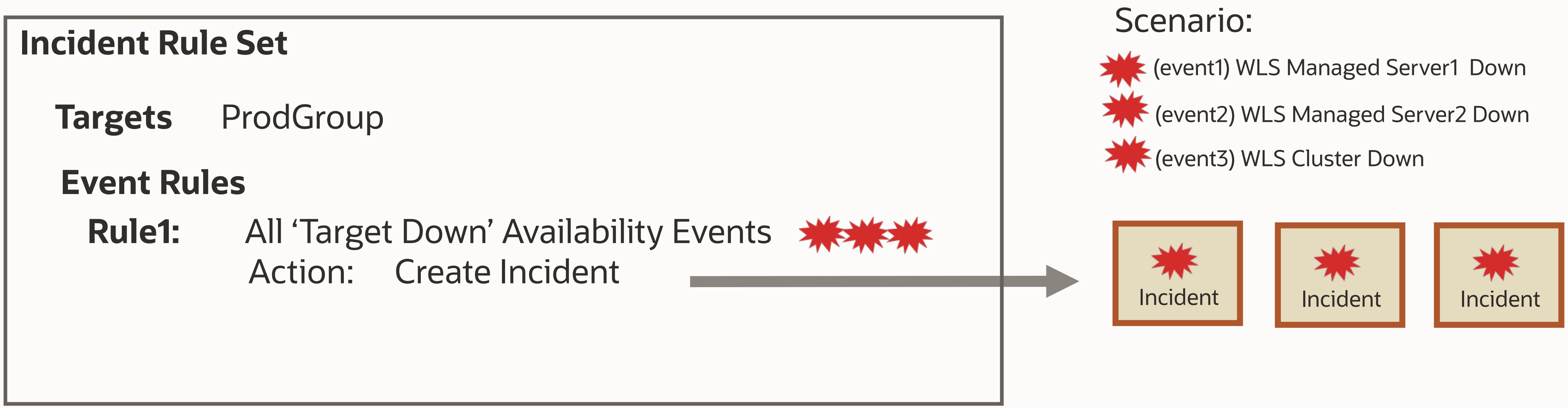
Event Compression Policies

- Event Compression Policy
  - Newer method of event compression introduced in Enterprise Manager Release Update (RU) 8
  - States the conditions under which to group multiple related events into 1 incident
    - Example:
      - Compress ’Target availability (i.e. down and error) events for the WebLogic cluster and its members’ if the events occur within a 5 minute time window
- Event compression policies are global
  - Applies to all incident-creating rules
  - Applicable policy will be applied, i.e., it matches the event type and targets of the rules
- 7 Out-of-box policies provided for common scenarios

Event Compression Policies

- Enabled out-of-the-box for new EM installations
  - Immediately applied to out-of-box rules
  - Users with specific privilege can disable/enable individual policies
    - Create Enterprise Ruleset privilege
- For upgraded EM sites
  - Auto enabled for new rules
  - For existing rules: user has to opt-in (enable) on per rule basis. Can do bulk-update.
    - To prevent changes in pre-existing incident creation/notification behavior after upgrading EM

Without Event Compression Policies



Incident Rule Set

Targets ProdGroup

Event Rules

Rule1: All ‘Target Down’ Availability Events

Action: Create Incident

Scenario:

(event1) WLS Managed Server1 Down

(event2) WLS Managed Server2 Down

(event3) WLS Cluster Down

With Event Compression Policies

For all event rules that create incidents: choose *Use Event Compression Policies*

Incident Rule Set

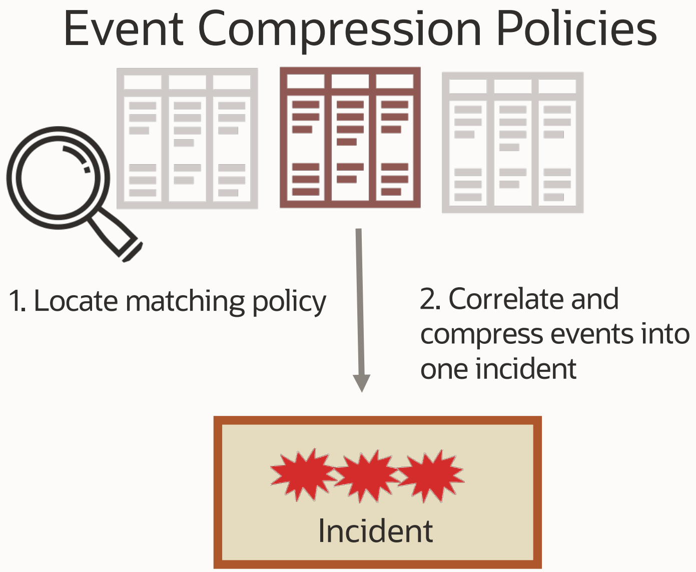
Targets ProdGroup

Event Rules

Rule1: All ‘Target Down’ Availability Events

Action: Create Incident

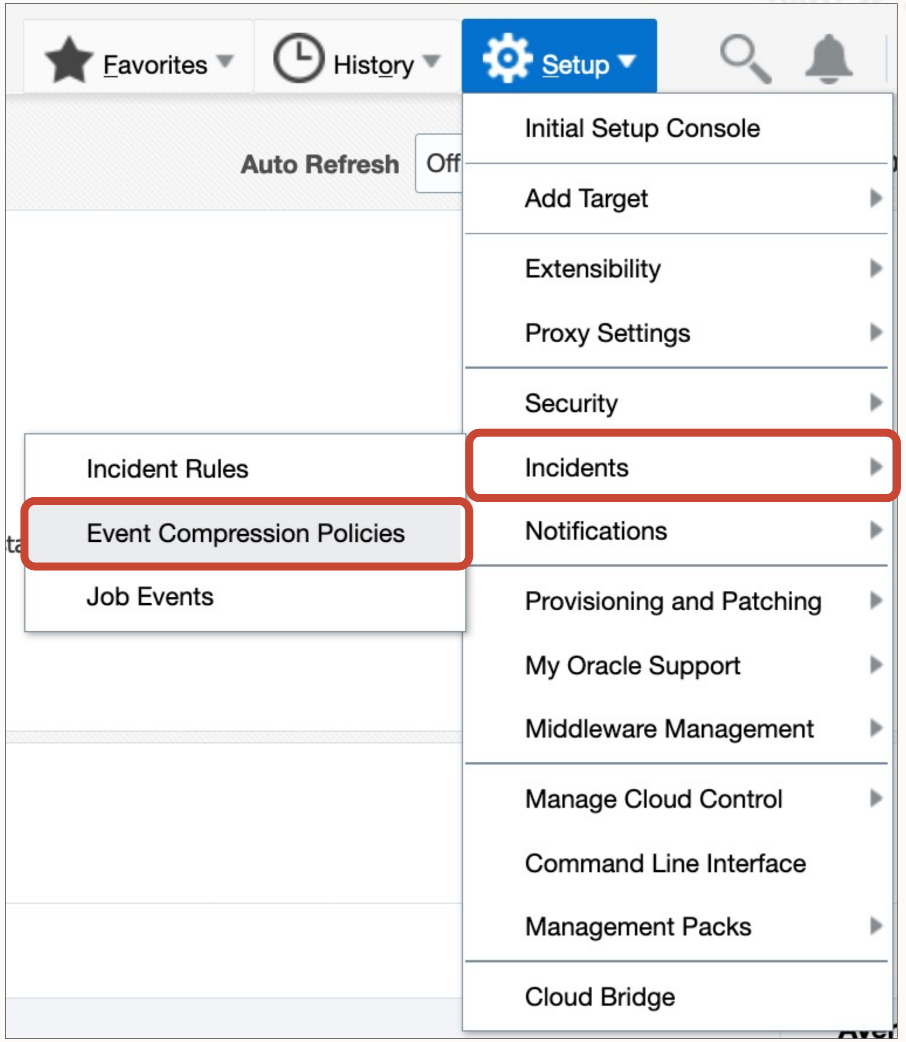
→ [✓] Use Event Compression Policies


Event Compression Policies
1. Locate matching policy
2. Correlate and compress events into one incident
Incident

Event Compression Policies

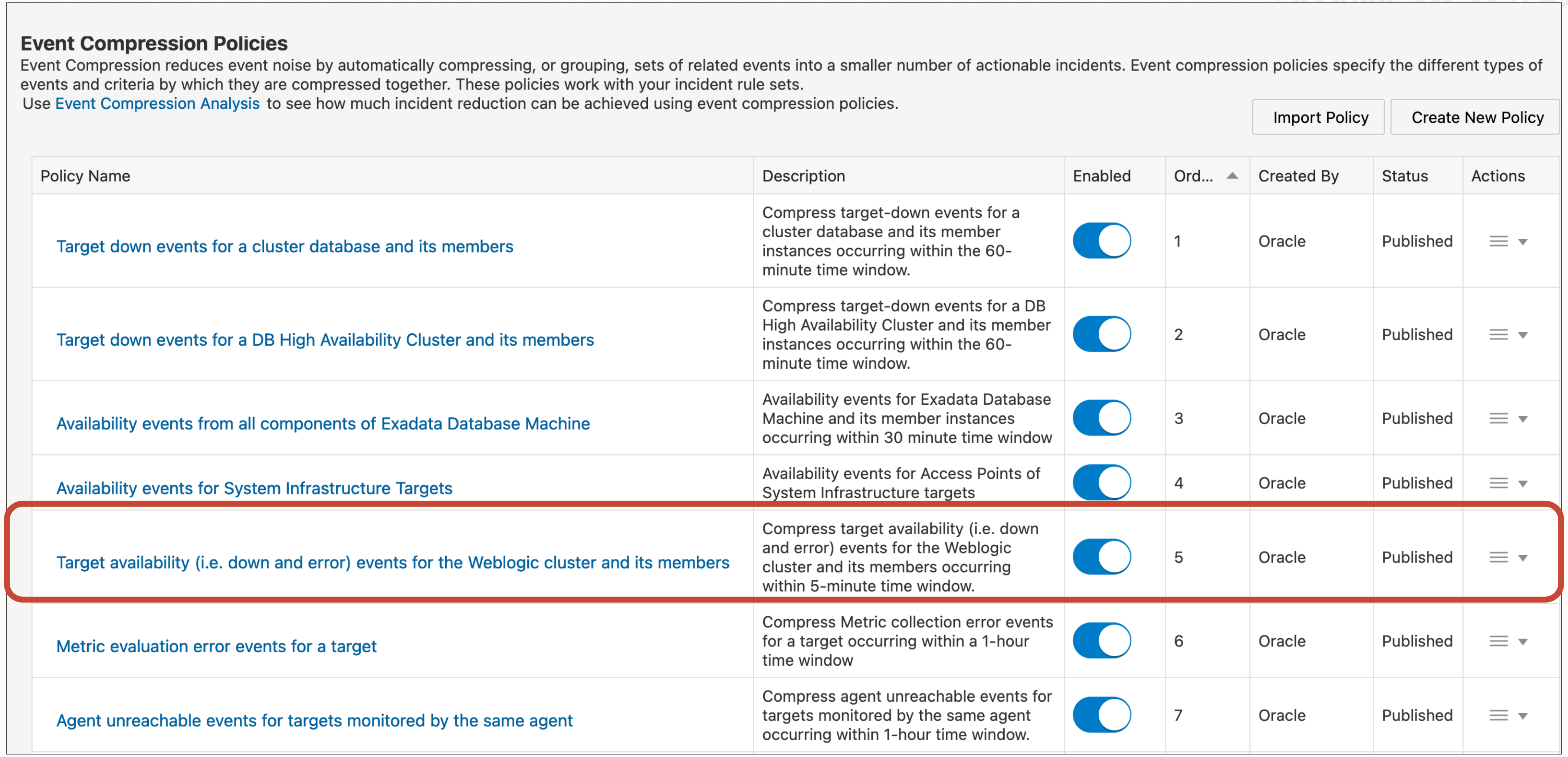
Navigating to Event Compression Policies

Setup > Incidents > Event Compression Policies



Event Compression Policies

Out-of-box policies



Event Compression Policies

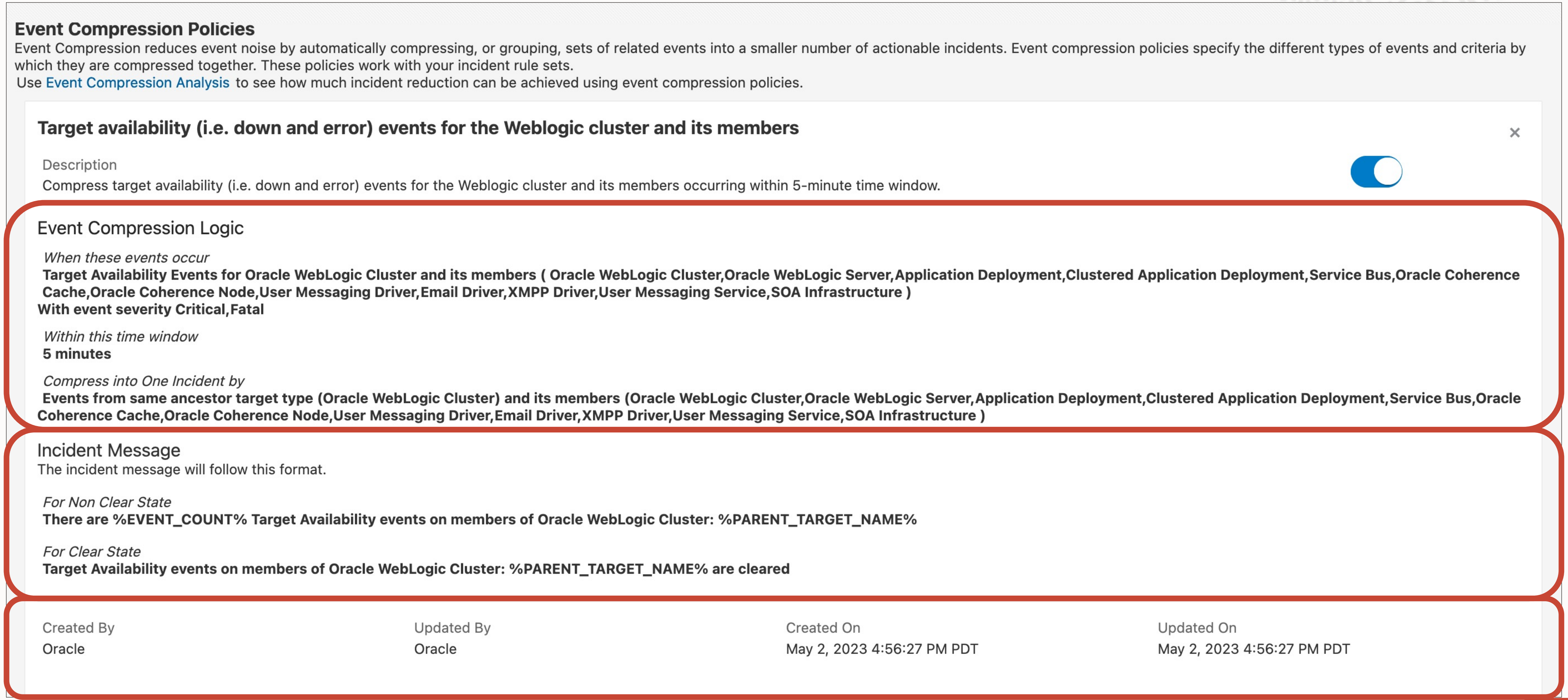
Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Policy Name	Description	Enabled	Ord... ▲	Created By	Status	Actions
Target down events for a cluster database and its members	Compress target-down events for a cluster database and its member instances occurring within the 60-minute time window.	●	1	Oracle	Published	≡ ▾
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	≡ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	≡ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	≡ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	≡ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	Published	≡ ▾
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	Published	≡ ▾

Event Compression Policies

Policy Definition



Event Compression Policies

Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Target availability (i.e. down and error) events for the Weblogic cluster and its members

Description

Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.

Event Compression Logic

When these events occur

Target Availability Events for Oracle WebLogic Cluster and its members (Oracle WebLogic Cluster,Oracle WebLogic Server,Application Deployment,Clustered Application Deployment,Service Bus,Oracle Coherence Cache,Oracle Coherence Node,User Messaging Driver,Email Driver,XMPP Driver,User Messaging Service,SOA Infrastructure)

With event severity Critical,Fatal

Within this time window

5 minutes

Compress into One Incident by

Events from same ancestor target type (Oracle WebLogic Cluster) and its members (Oracle WebLogic Cluster,Oracle WebLogic Server,Application Deployment,Clustered Application Deployment,Service Bus,Oracle Coherence Cache,Oracle Coherence Node,User Messaging Driver,Email Driver,XMPP Driver,User Messaging Service,SOA Infrastructure)

Incident Message

The incident message will follow this format.

For Non Clear State

There are %EVENT_COUNT% Target Availability events on members of Oracle WebLogic Cluster: %PARENT_TARGET_NAME%

For Clear State

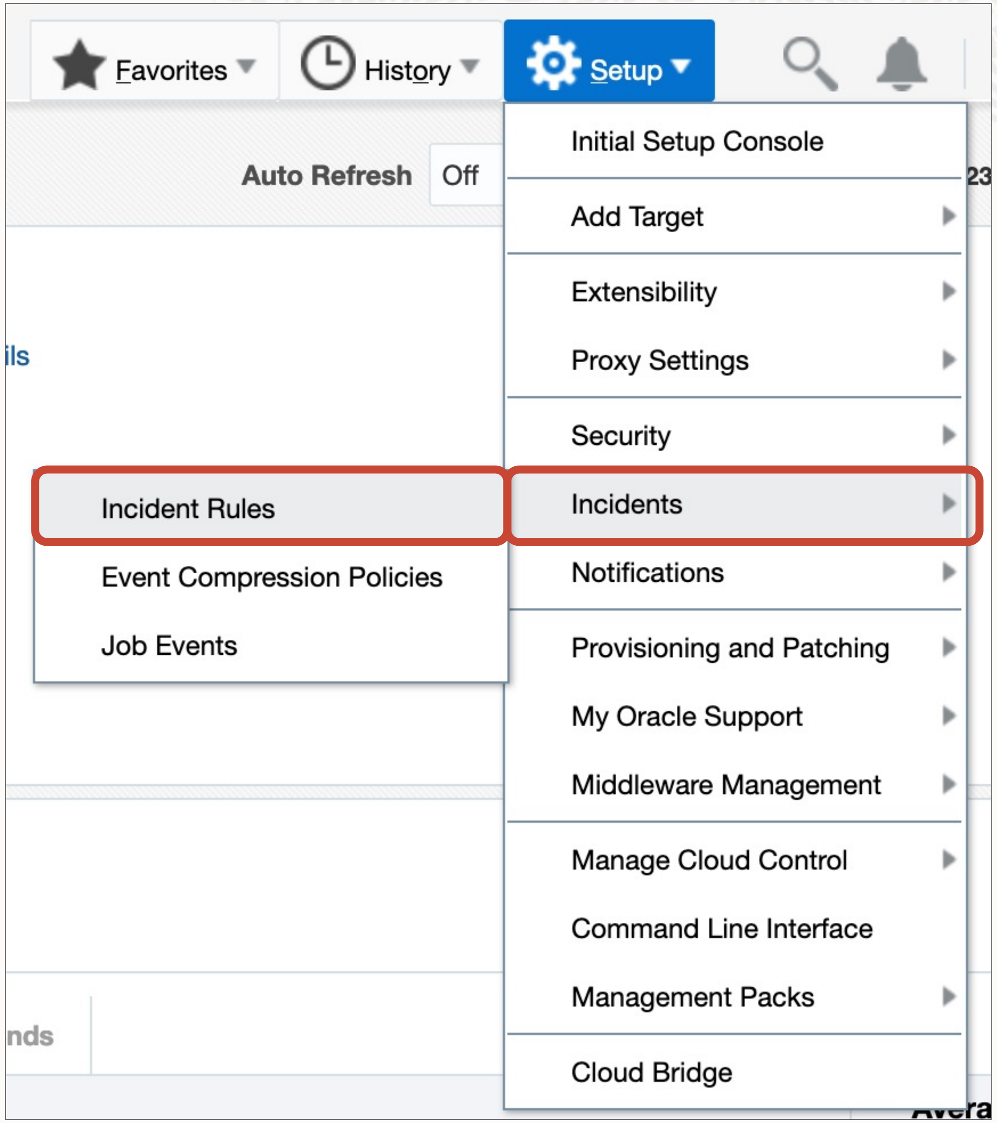
Target Availability events on members of Oracle WebLogic Cluster: %PARENT_TARGET_NAME% are cleared

Created By	Updated By	Created On	Updated On
Oracle	Oracle	May 2, 2023 4:56:27 PM PDT	May 2, 2023 4:56:27 PM PDT

Event Compression Policies

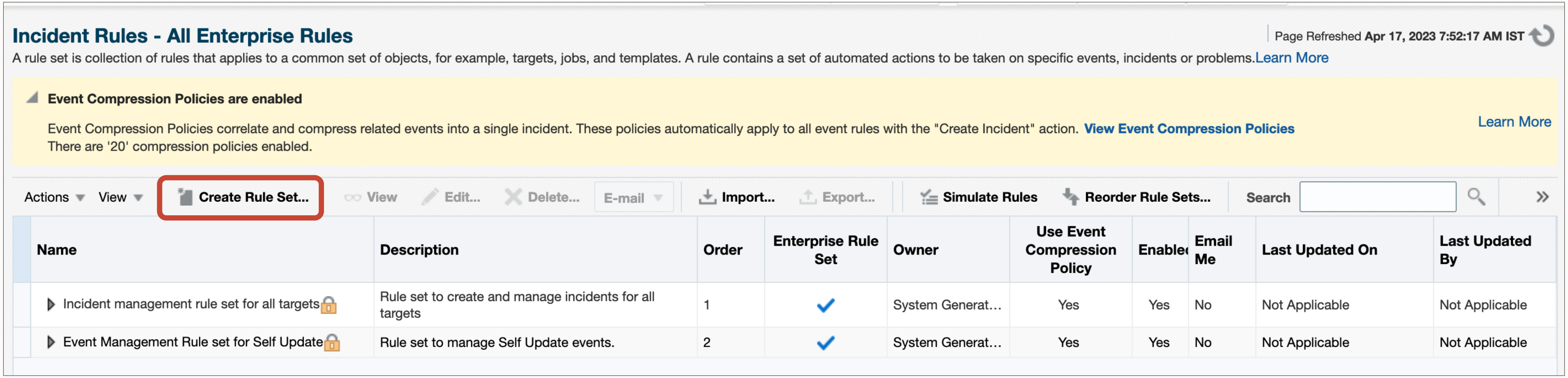
Navigating to Incident Rules

Setup > Incident > Incident Rules



Event Compression Policies

Incident Rules - Create Rule Set



Incident Rules - All Enterprise Rules

Page Refreshed Apr 17, 2023 7:52:17 AM IST

A rule set is collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. Learn More

Event Compression Policies are enabled

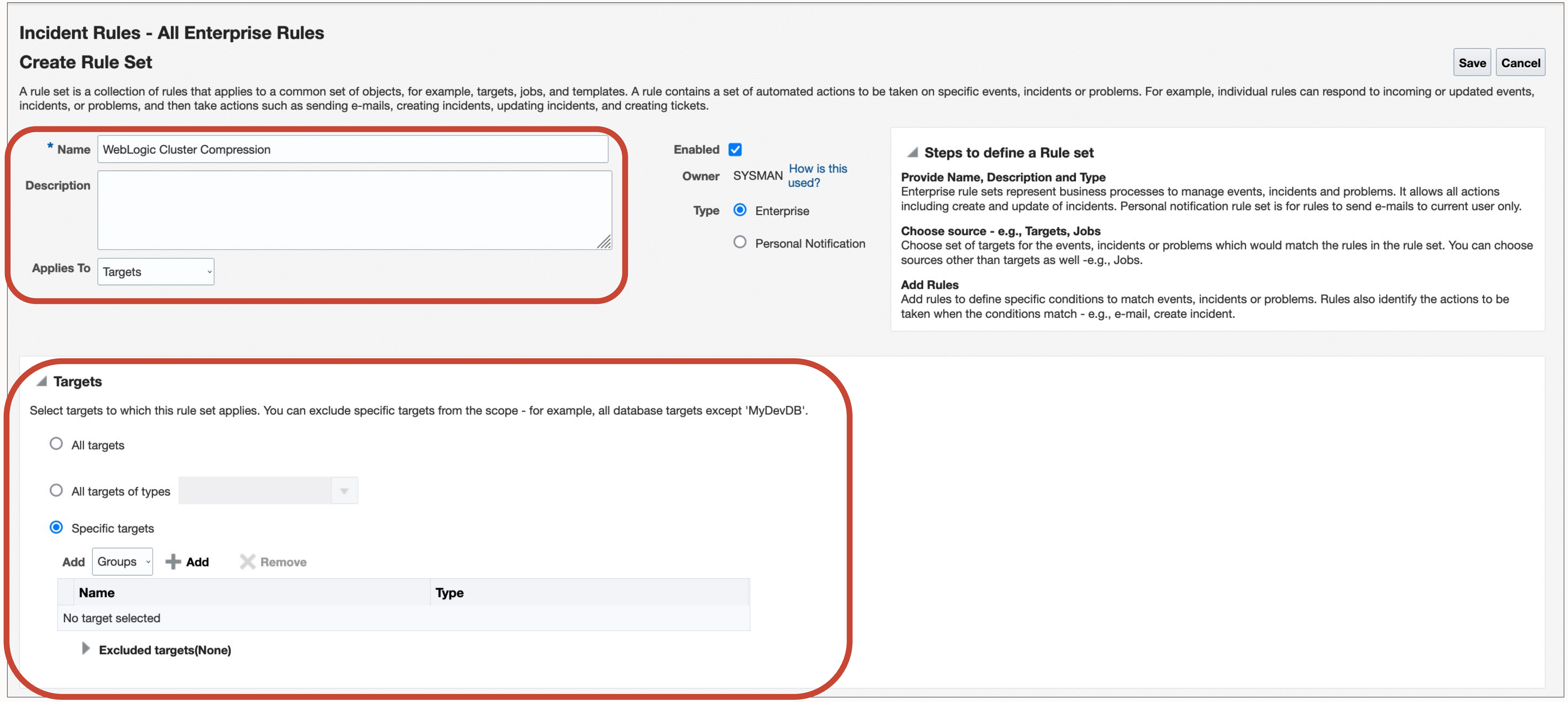
Event Compression Policies correlate and compress related events into a single incident. These policies automatically apply to all event rules with the "Create Incident" action. **View Event Compression Policies**
There are '20' compression policies enabled.

Learn More

Name	Description	Order	Enterprise Rule Set	Owner	Use Event Compression Policy	Enablec	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat…	Yes	Yes	No	Not Applicable	Not Applicable
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat…	Yes	Yes	No	Not Applicable	Not Applicable

Event Compression Policies

Incident Rules - Specify the name of rule set and select targets to apply on



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: WebLogic Cluster Compression

Description:

Applies To: Targets

Enabled ☑

Owner: SYSMAN

Type: ● Enterprise ○ Personal Notification

Steps to define a Rule set

Provide Name, Description and Type
Enterprise rule sets represent business processes to manage events, incidents and problems. It allows all actions including create and update of incidents. Personal notification rule set is for rules to send e-mails to current user only.

Choose source - e.g., Targets, Jobs
Choose set of targets for the events, incidents or problems which would match the rules in the rule set. You can choose sources other than targets as well -e.g., Jobs.

Add Rules
Add rules to define specific conditions to match events, incidents or problems. Rules also identify the actions to be taken when the conditions match - e.g., e-mail, create incident.

Targets

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except 'MyDevDB'.

○ All targets

○ All targets of types

● Specific targets

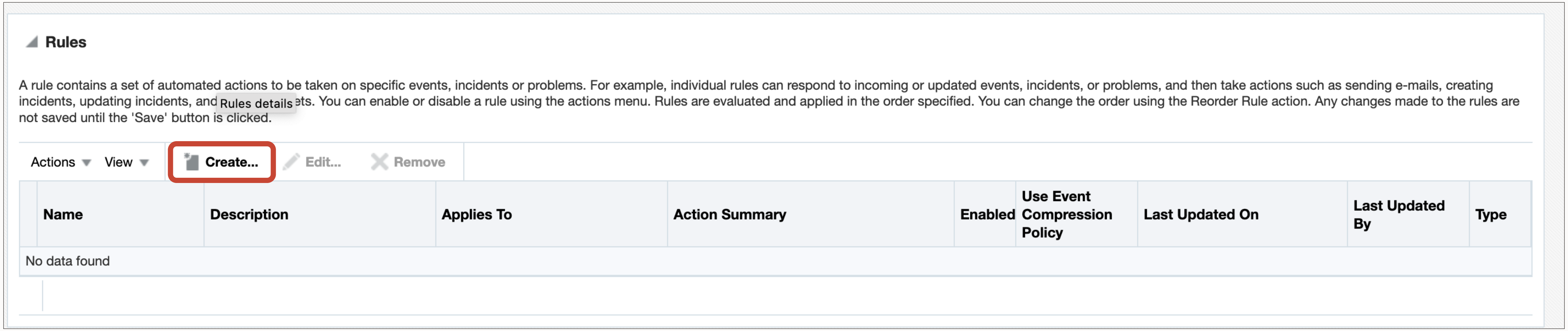
Add: Groups

Name	Type
No target selected	

Excluded targets(None)

Event Compression Policies

Incident Rules – Create rule



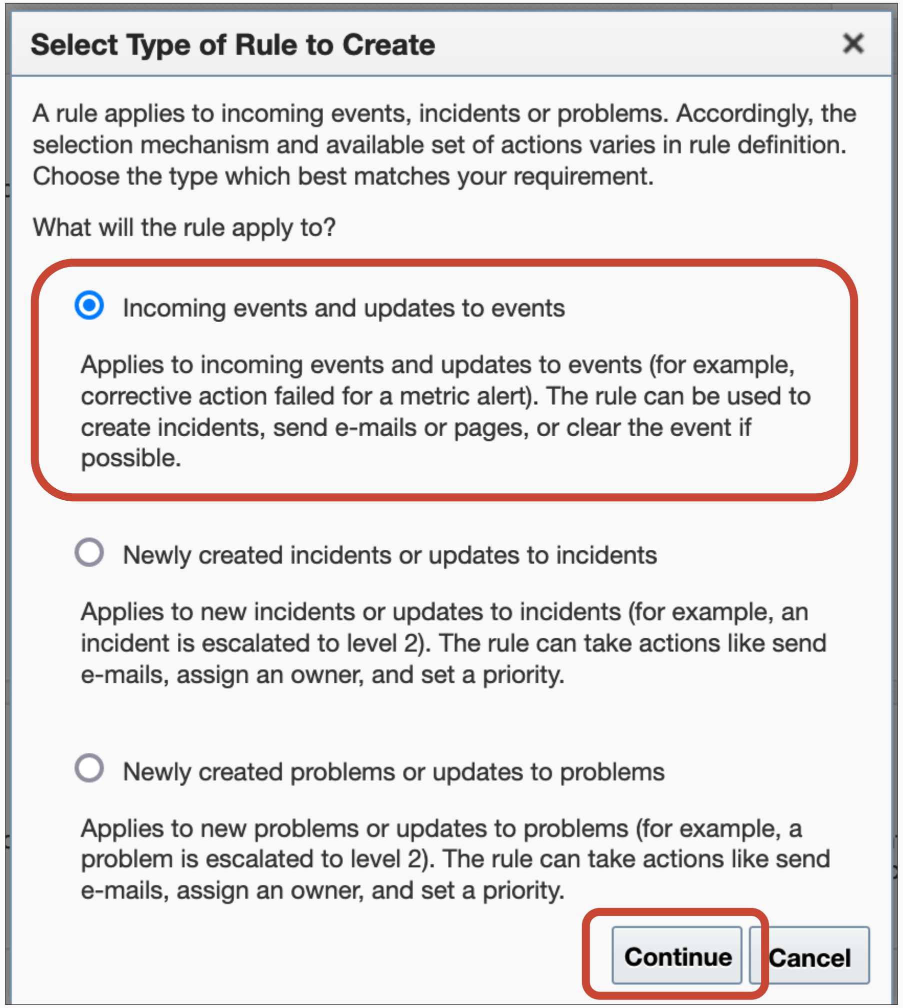
◢ Rules

A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and Rules details ets. You can enable or disable a rule using the actions menu. Rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule action. Any changes made to the rules are not saved until the 'Save' button is clicked.

Name	Description	Applies To	Action Summary	Enabled	Use Event Compression Policy	Last Updated On	Last Updated By	Type
No data found								

Event Compression Policies

Incident Rules – Select for incoming events



Select Type of Rule to Create ✕

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

What will the rule apply to?

● Incoming events and updates to events

Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

○ Newly created incidents or updates to incidents

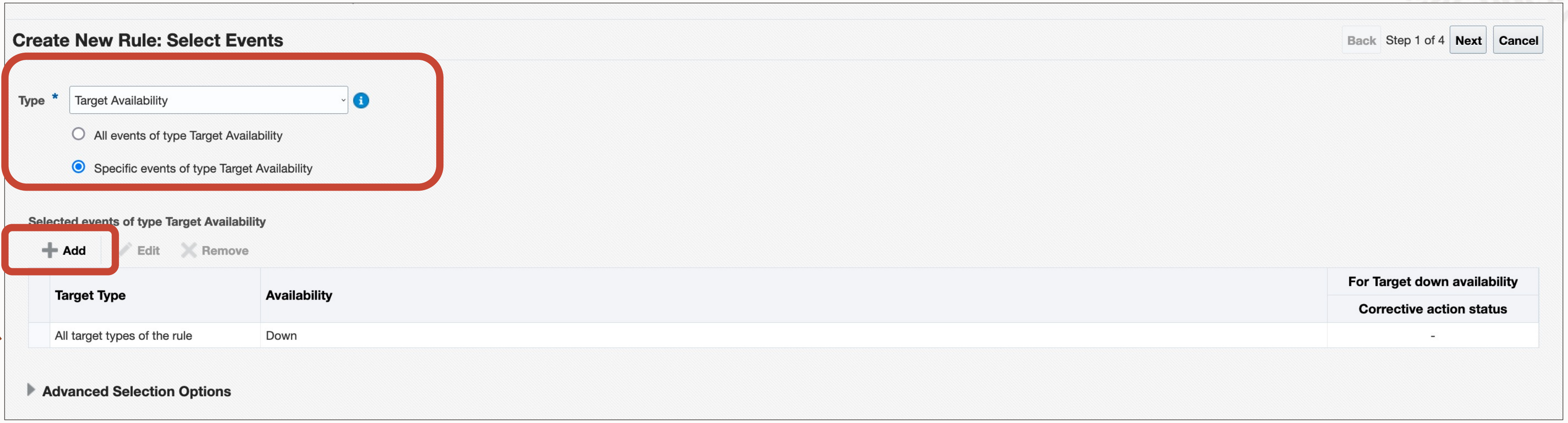
Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

○ Newly created problems or updates to problems

Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

Event Compression Policies

Incident Rules - Select event types



Create New Rule: Select Events

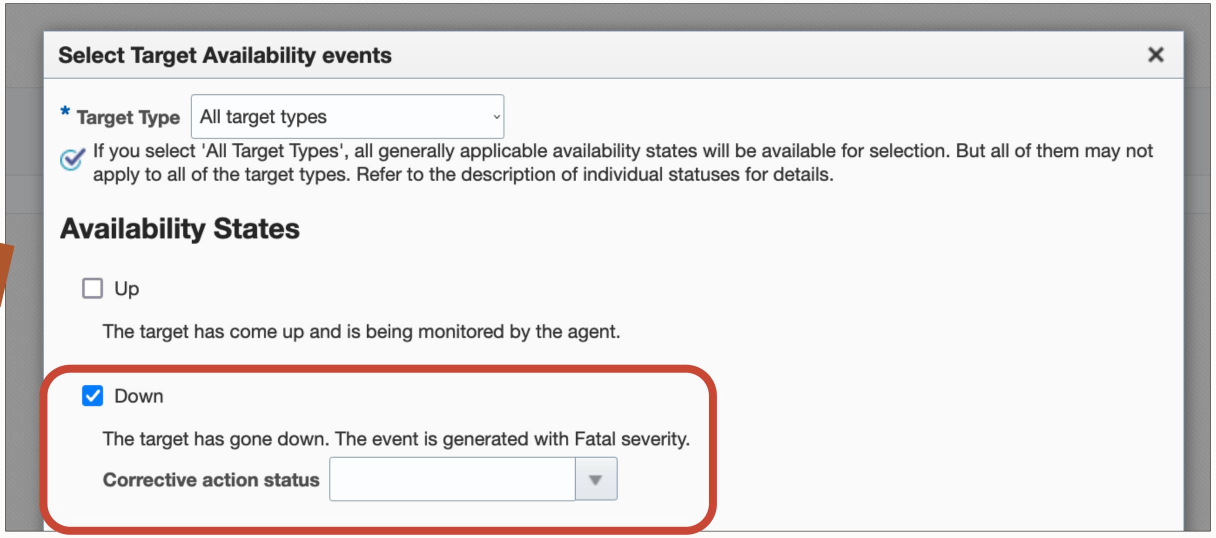
Type * Target Availability

○ All events of type Target Availability

● Specific events of type Target Availability

Selected events of type Target Availability

Target Type	Availability	For Target down availability Corrective action status
All target types of the rule	Down	-



Select Target Availability events ×

* Target Type: All target types

If you select 'All Target Types', all generally applicable availability states will be available for selection. But all of them may not apply to all of the target types. Refer to the description of individual statuses for details.

Availability States

□ Up

The target has come up and is being monitored by the agent.

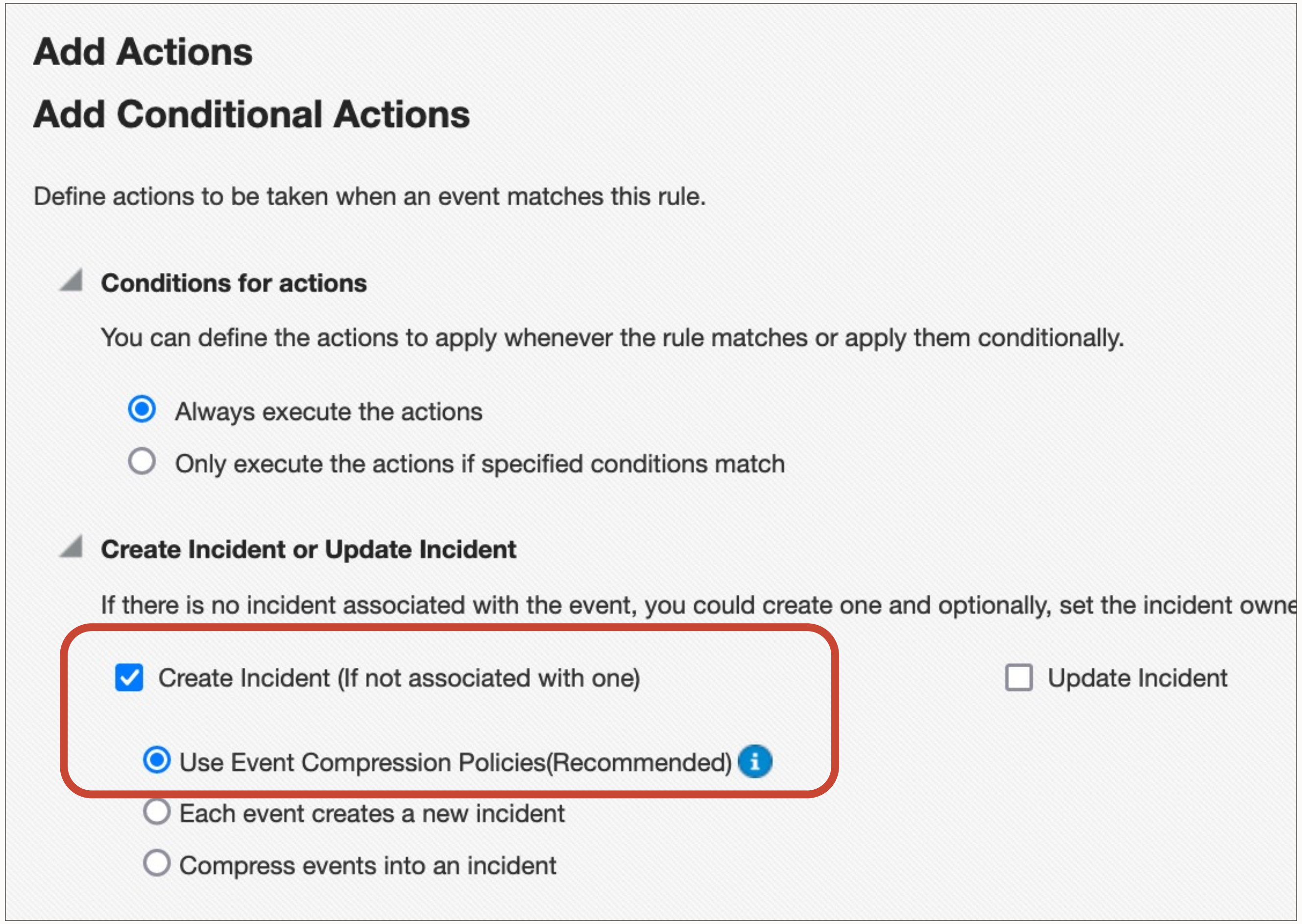
☑ Down

The target has gone down. The event is generated with Fatal severity.

Corrective action status

Event Compression Policies

Incident Rules - Add Actions (enable policy use)



Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

● Always execute the actions

○ Only execute the actions if specified conditions match

Create Incident or Update Incident

If there is no incident associated with the event, you could create one and optionally, set the incident owne

☑ Create Incident (If not associated with one) □ Update Incident

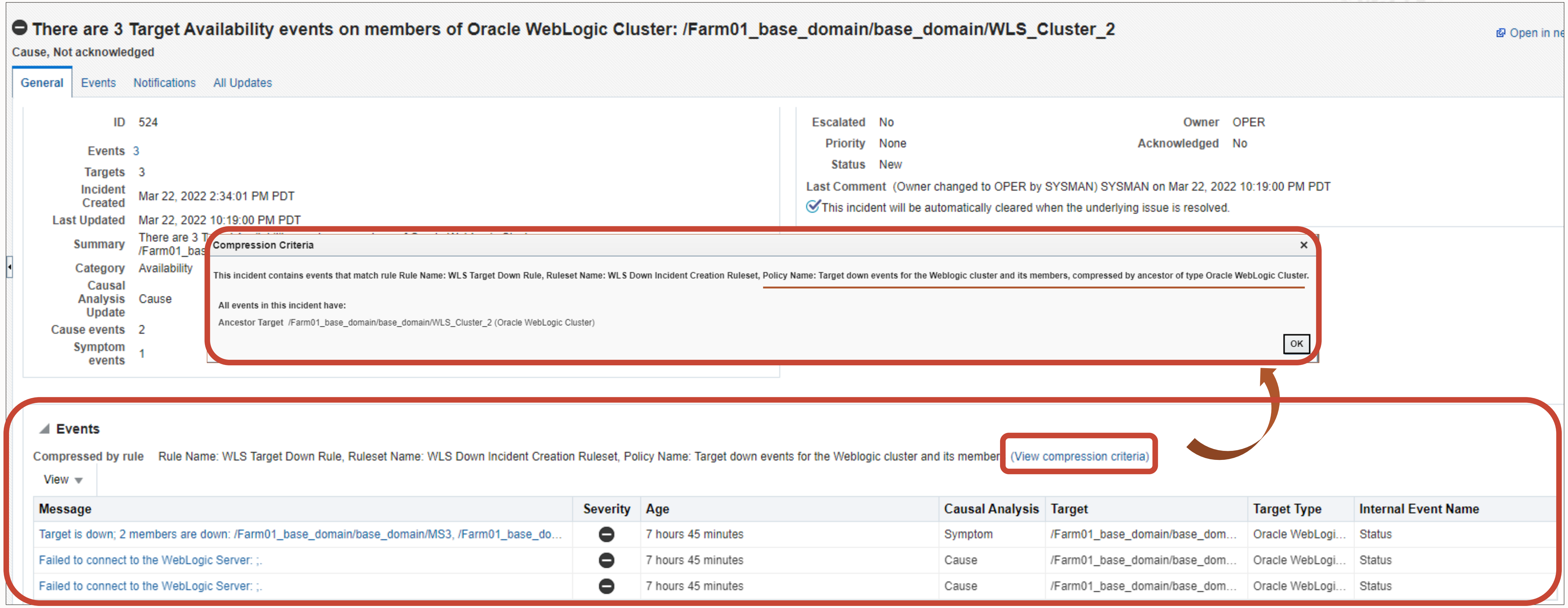
● Use Event Compression Policies(Recommended)

○ Each event creates a new incident

○ Compress events into an incident

Event Compression Policies

Incident with 3 compressed events



There are 3 Target Availability events on members of Oracle WebLogic Cluster: /Farm01_base_domain/base_domain/WLS_Cluster_2

Cause, Not acknowledged

ID	524
Events	3
Targets	3
Incident Created	Mar 22, 2022 2:34:01 PM PDT
Last Updated	Mar 22, 2022 10:19:00 PM PDT
Summary	There are 3 T /Farm01_bas
Category	Availability
Causal Analysis Update	Cause
Cause events	2
Symptom events	1

Escalated	No	Owner	OPER
Priority	None	Acknowledged	No
Status	New		

Last Comment (Owner changed to OPER by SYSMAN) SYSMAN on Mar 22, 2022 10:19:00 PM PDT

✓ This incident will be automatically cleared when the underlying issue is resolved.

Compression Criteria

This incident contains events that match rule Rule Name: WLS Target Down Rule, Ruleset Name: WLS Down Incident Creation Ruleset, Policy Name: Target down events for the Weblogic cluster and its members, compressed by ancestor of type Oracle WebLogic Cluster.

All events in this incident have:

Ancestor Target /Farm01_base_domain/base_domain/WLS_Cluster_2 (Oracle WebLogic Cluster)

Events

Compressed by rule Rule Name: WLS Target Down Rule, Ruleset Name: WLS Down Incident Creation Ruleset, Policy Name: Target down events for the Weblogic cluster and its member (View compression criteria)

Message	Severity	Age	Causal Analysis	Target	Target Type	Internal Event Name
Target is down; 2 members are down: /Farm01_base_domain/base_domain/MS3, /Farm01_base_do...	⊖	7 hours 45 minutes	Symptom	/Farm01_base_domain/base_dom...	Oracle WebLogi...	Status
Failed to connect to the WebLogic Server: ;.	⊖	7 hours 45 minutes	Cause	/Farm01_base_domain/base_dom...	Oracle WebLogi...	Status
Failed to connect to the WebLogic Server: ;.	⊖	7 hours 45 minutes	Cause	/Farm01_base_domain/base_dom...	Oracle WebLogi...	Status

Use Event Compression to reduce event noise

- Event Compression
- User-Defined Event Compression Policies
- Event Compression Analysis

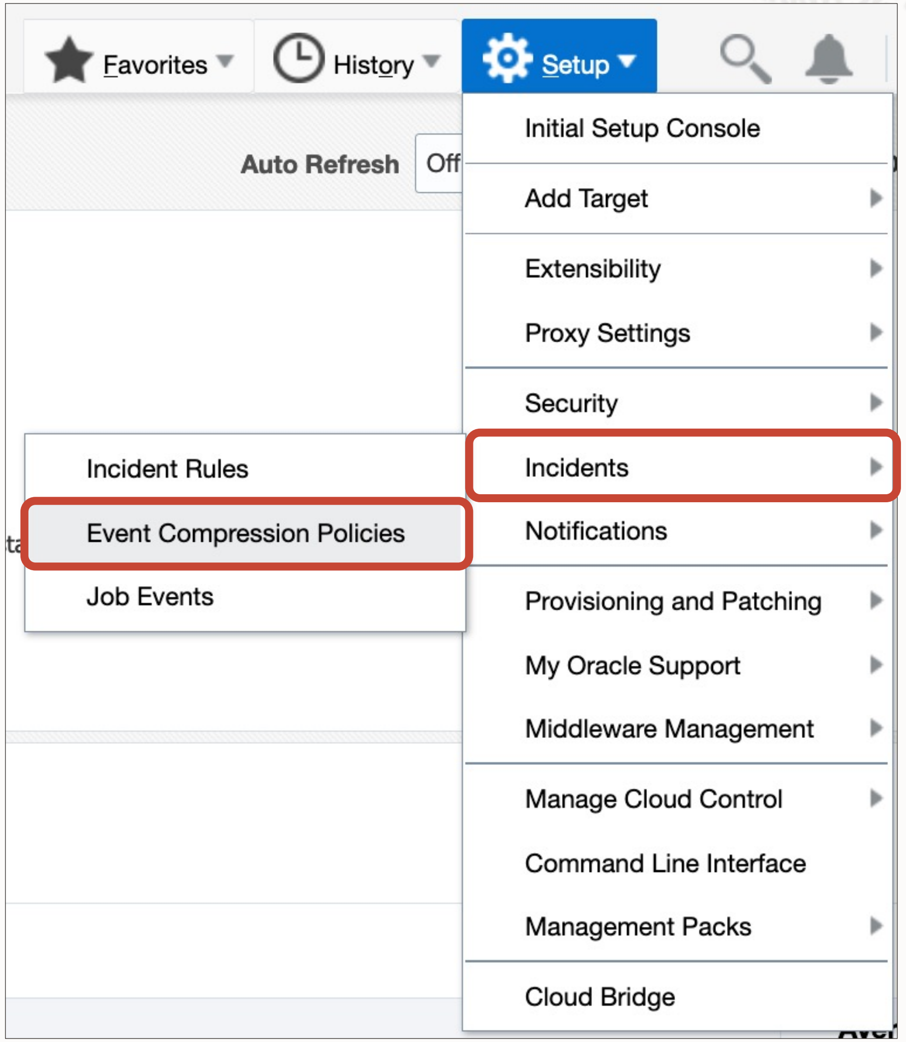
User-Defined Event Compression Policies

- Option to create a *user-defined event compression policy*
  - Users can author their own policies that will apply to all incident-creating rules
- Useful if the OOB policies do not fit ones use case
- To create, update, or delete a user-defined event compression policy, you must have *Create Business Rule* privilege
- User-Defined policies can be published and used by other administrators

User-Defined Policies

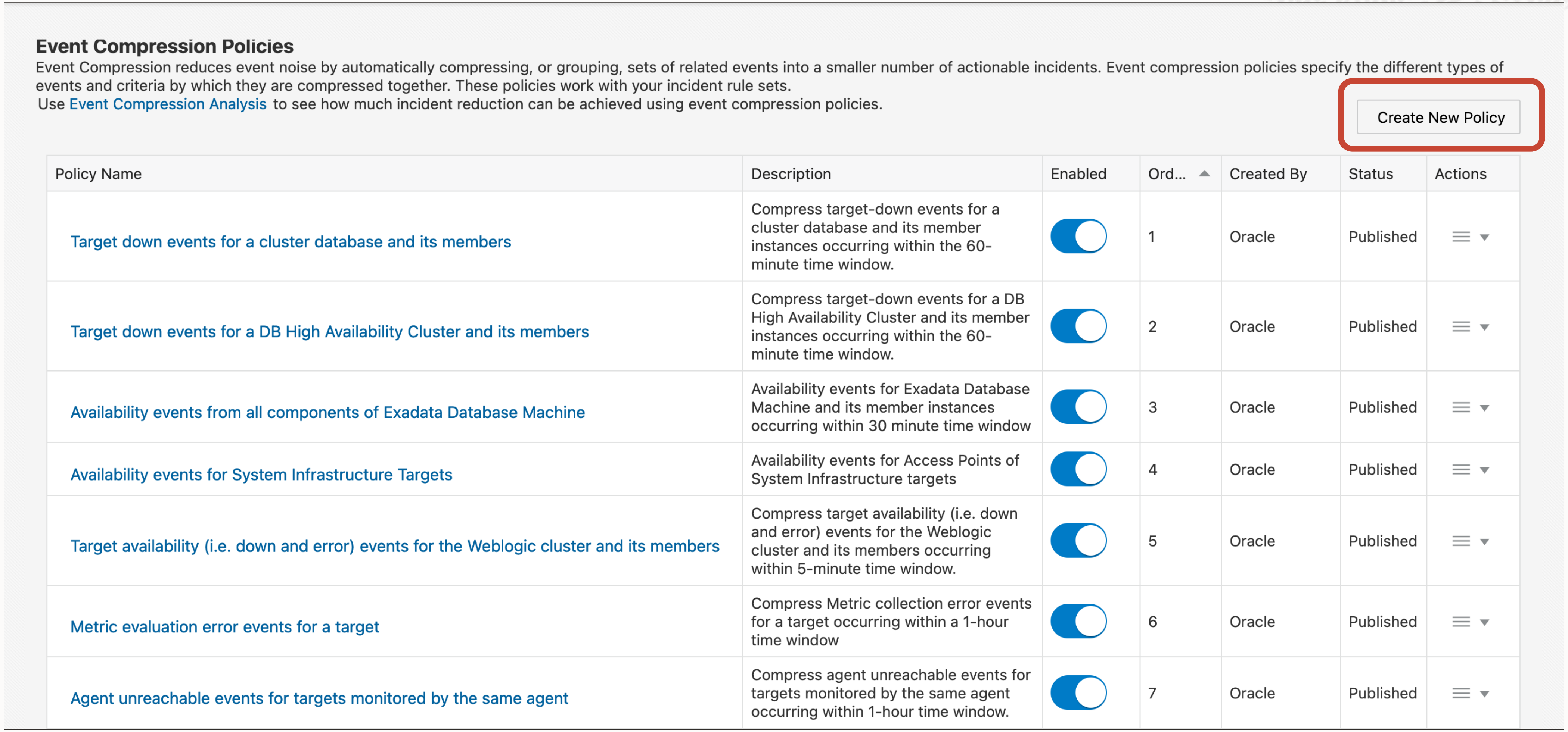
Navigating to Event Compression Policies

Setup > Incidents > Event Compression Policies



User-Defined Policies

Event Compression Policies



Event Compression Policies

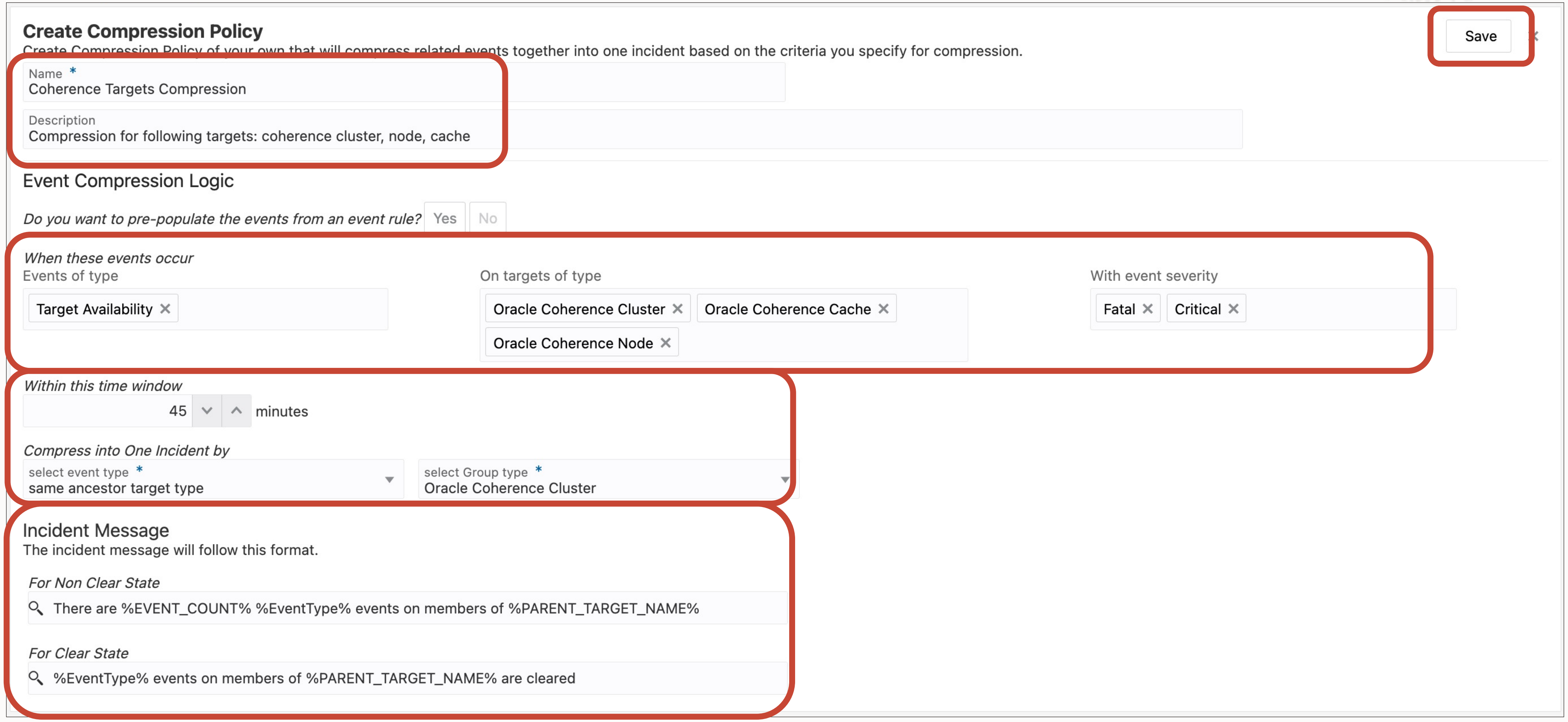
Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Policy Name	Description	Enabled	Ord... ▲	Created By	Status	Actions
Target down events for a cluster database and its members	Compress target-down events for a cluster database and its member instances occurring within the 60-minute time window.	●	1	Oracle	Published	≡ ▾
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	≡ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	≡ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	≡ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	≡ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	Published	≡ ▾
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	Published	≡ ▾

User-Defined Policies

Create compression policy



Create Compression Policy

Create Compression Policy of your own that will compress related events together into one incident based on the criteria you specify for compression.

Name *
Coherence Targets Compression

Description
Compression for following targets: coherence cluster, node, cache

Event Compression Logic

Do you want to pre-populate the events from an event rule? Yes No

When these events occur

Events of type: Target Availability ✕

On targets of type: Oracle Coherence Cluster ✕ Oracle Coherence Cache ✕ Oracle Coherence Node ✕

With event severity: Fatal ✕ Critical ✕

Within this time window
45 minutes

Compress into One Incident by

select event type *
same ancestor target type

select Group type *
Oracle Coherence Cluster

Incident Message

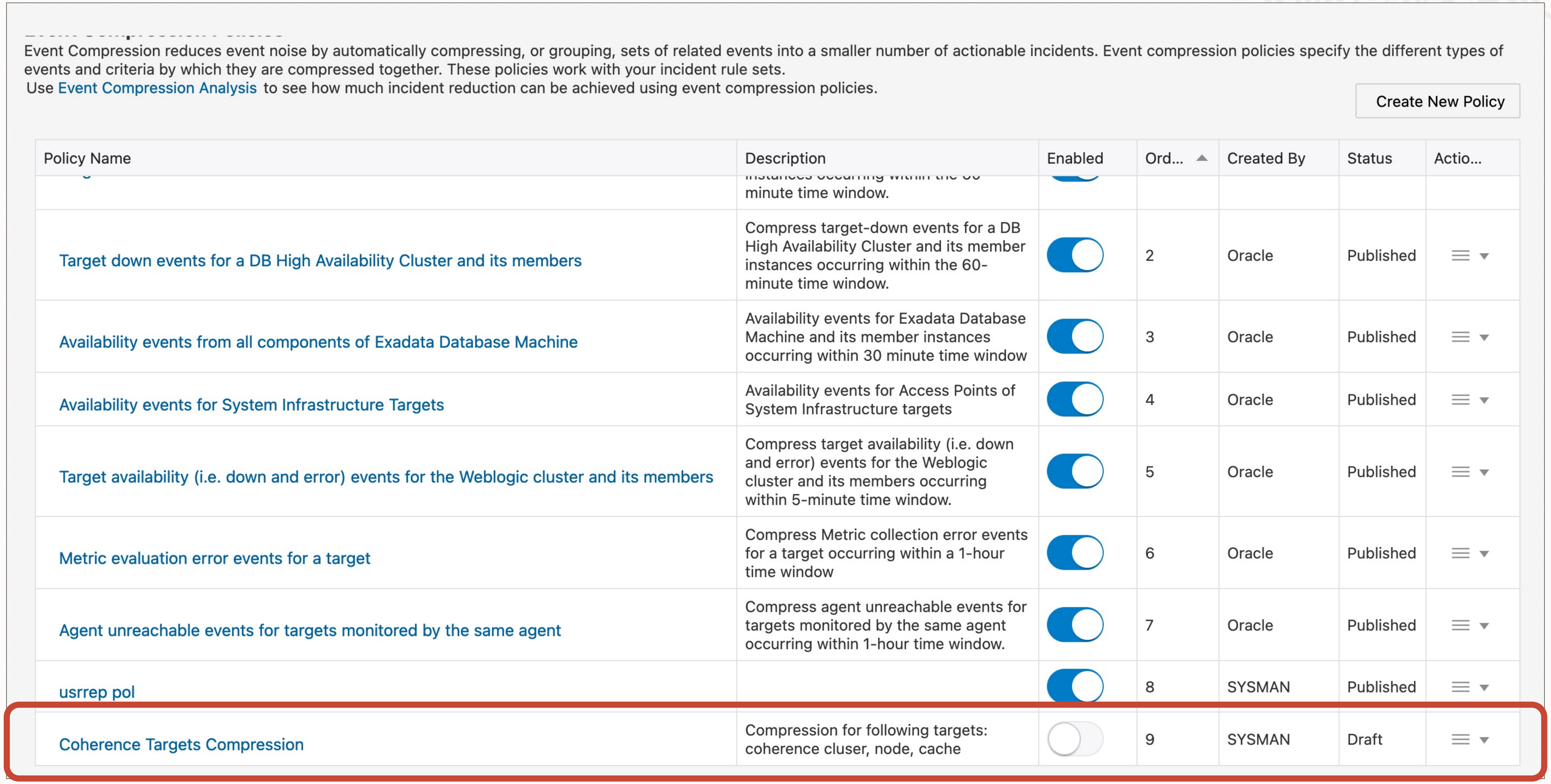
The incident message will follow this format.

For Non Clear State
There are %EVENT_COUNT% %EventType% events on members of %PARENT_TARGET_NAME%

For Clear State
%EventType% events on members of %PARENT_TARGET_NAME% are cleared

User-Defined Policies

Policy created



Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

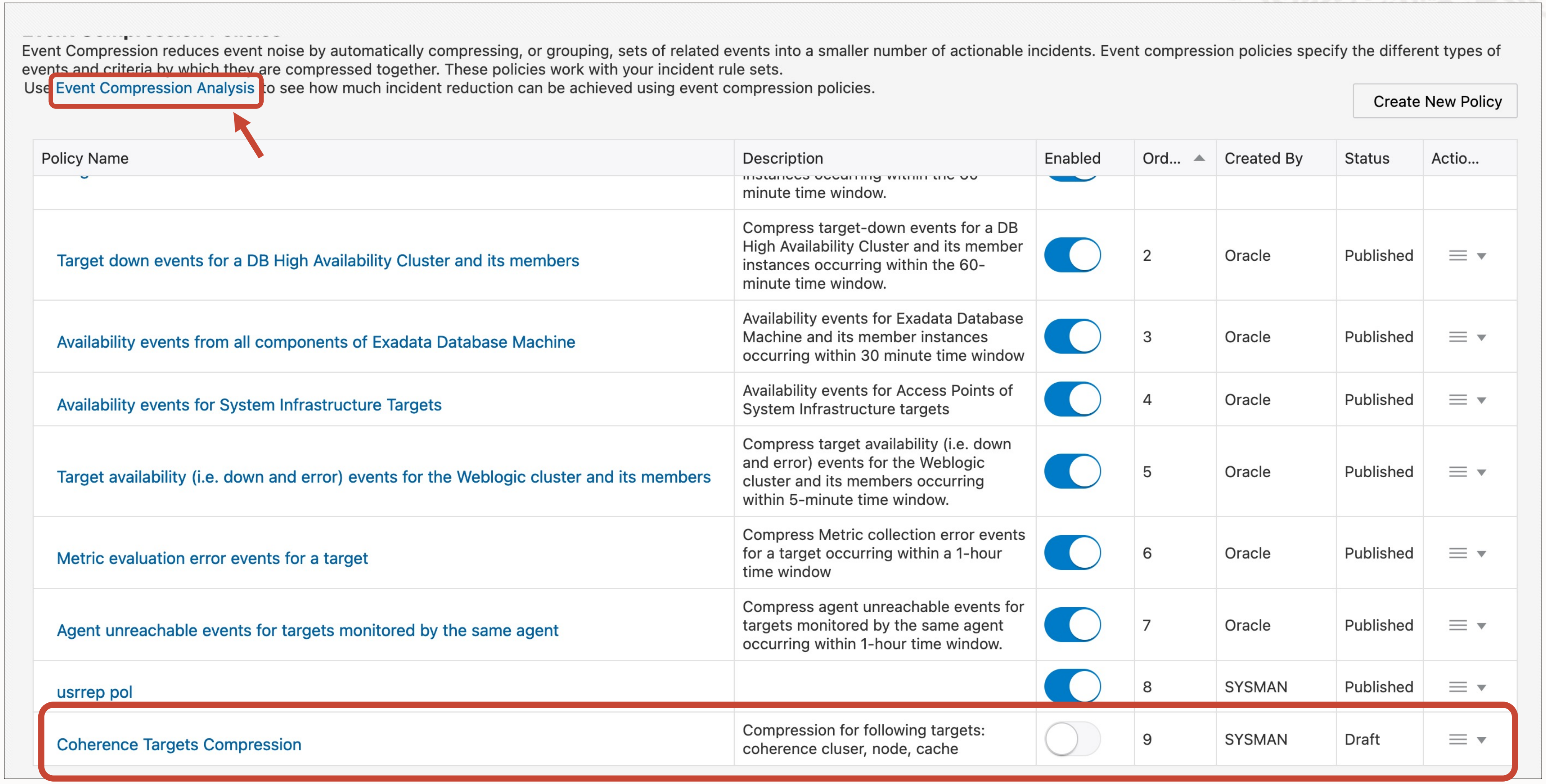
Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Create New Policy

Policy Name	Description	Enabled	Ord... ▲	Created By	Status	Actio...
	minute time window.					
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	≡ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	≡ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	≡ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	≡ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	Published	≡ ▾
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	Published	≡ ▾
usrrep pol		●	8	SYSMAN	Published	≡ ▾
Coherence Targets Compression	Compression for following targets: coherence cluser, node, cache	○	9	SYSMAN	Draft	≡ ▾

Testing the User-Defined Policy

Event Compression Analysis



Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.
Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Policy Name	Description	Enabled	Ord... ▲	Created By	Status	Actio...
	minute time window.					
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	≡ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	≡ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	≡ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	≡ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	Published	≡ ▾
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	Published	≡ ▾
usrrep pol		●	8	SYSMAN	Published	≡ ▾
Coherence Targets Compression	Compression for following targets: coherence cluser, node, cache	○	9	SYSMAN	Draft	≡ ▾

Use Event Compression to reduce event noise

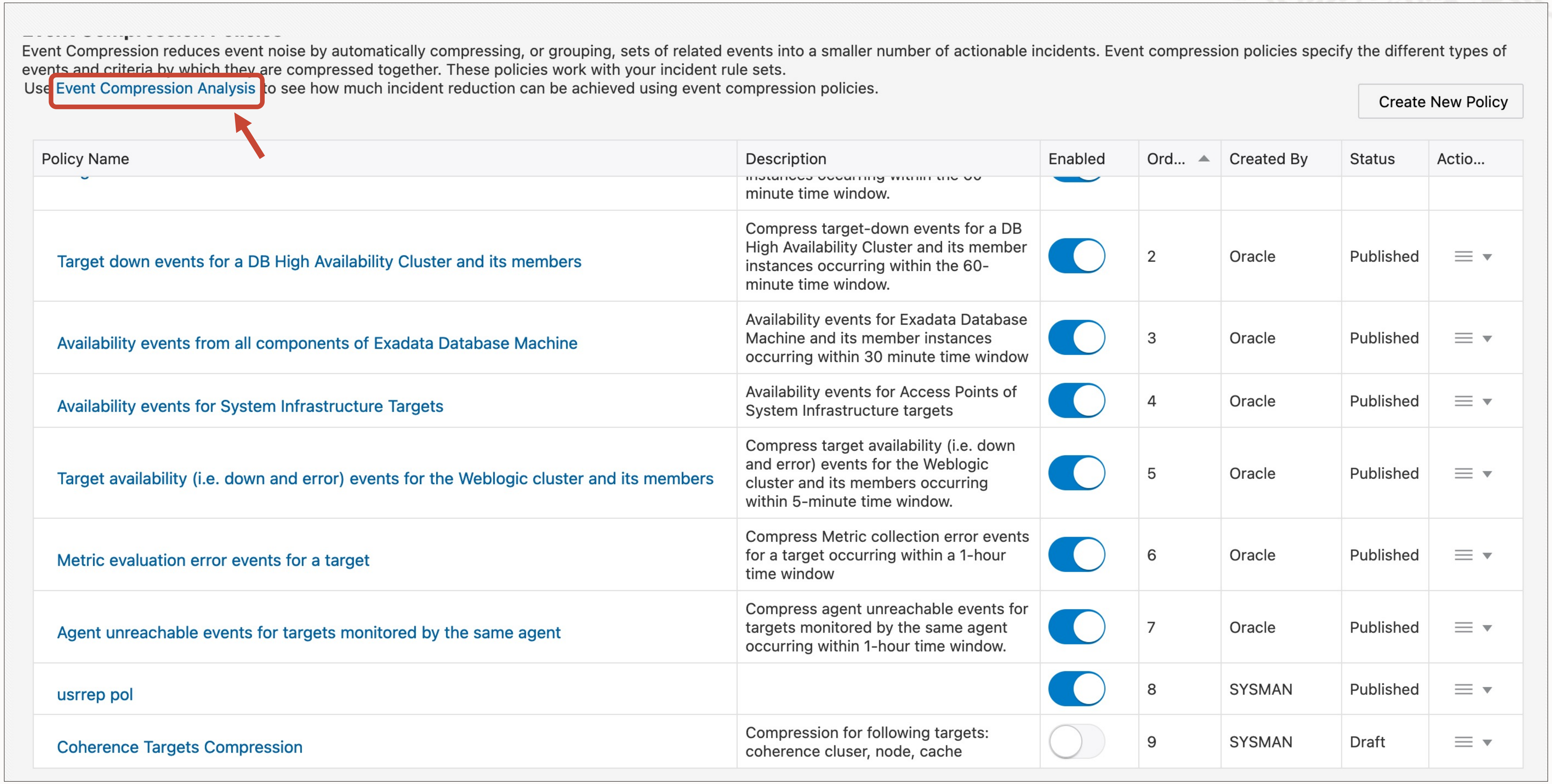
- Event Compression
- User-Defined Event Compression Policies
- Event Compression Analysis

Event Compression Analysis

- To help users understand the benefit of event compression policies
- Useful for testing draft policies
- Event compression will be simulated using the user’s own events data (e.g. last 30 days)
- Users can compare:
  - Number of incidents in last month vs. (smaller) number of incidents with event compression enabled
- Users can run these analysis reports on demand

Event Compression Analysis

Navigate to analysis



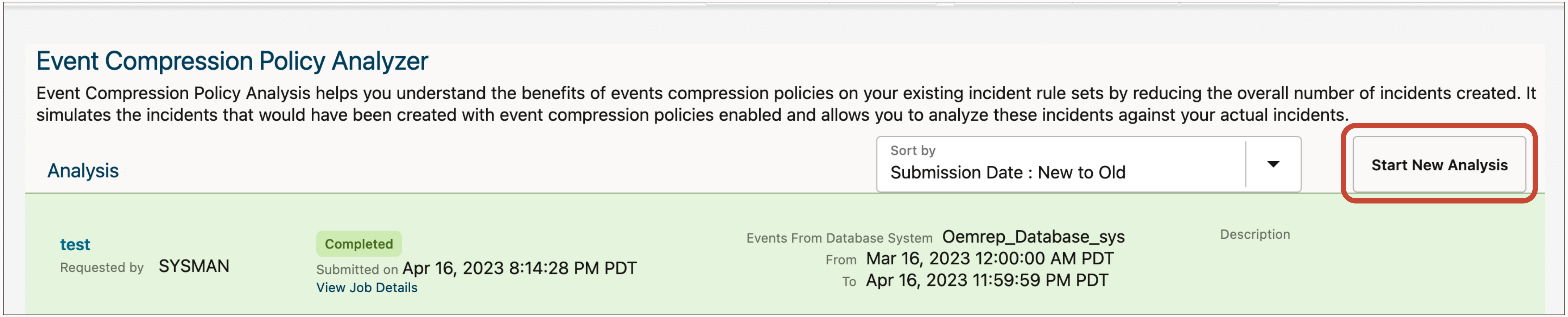
Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Policy Name	Description	Enabled	Ord... ▲	Created By	Status	Actio...
	minute time window.					
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	≡ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	≡ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	≡ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	≡ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	Published	≡ ▾
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	Published	≡ ▾
usrrep pol		●	8	SYSMAN	Published	≡ ▾
Coherence Targets Compression	Compression for following targets: coherence cluser, node, cache	○	9	SYSMAN	Draft	≡ ▾

Event Compression Analysis

Analysis homepage



Event Compression Policy Analyzer

Event Compression Policy Analysis helps you understand the benefits of events compression policies on your existing incident rule sets by reducing the overall number of incidents created. It simulates the incidents that would have been created with event compression policies enabled and allows you to analyze these incidents against your actual incidents.

Analysis

Sort by: Submission Date : New to Old

test
Requested by SYSMAN

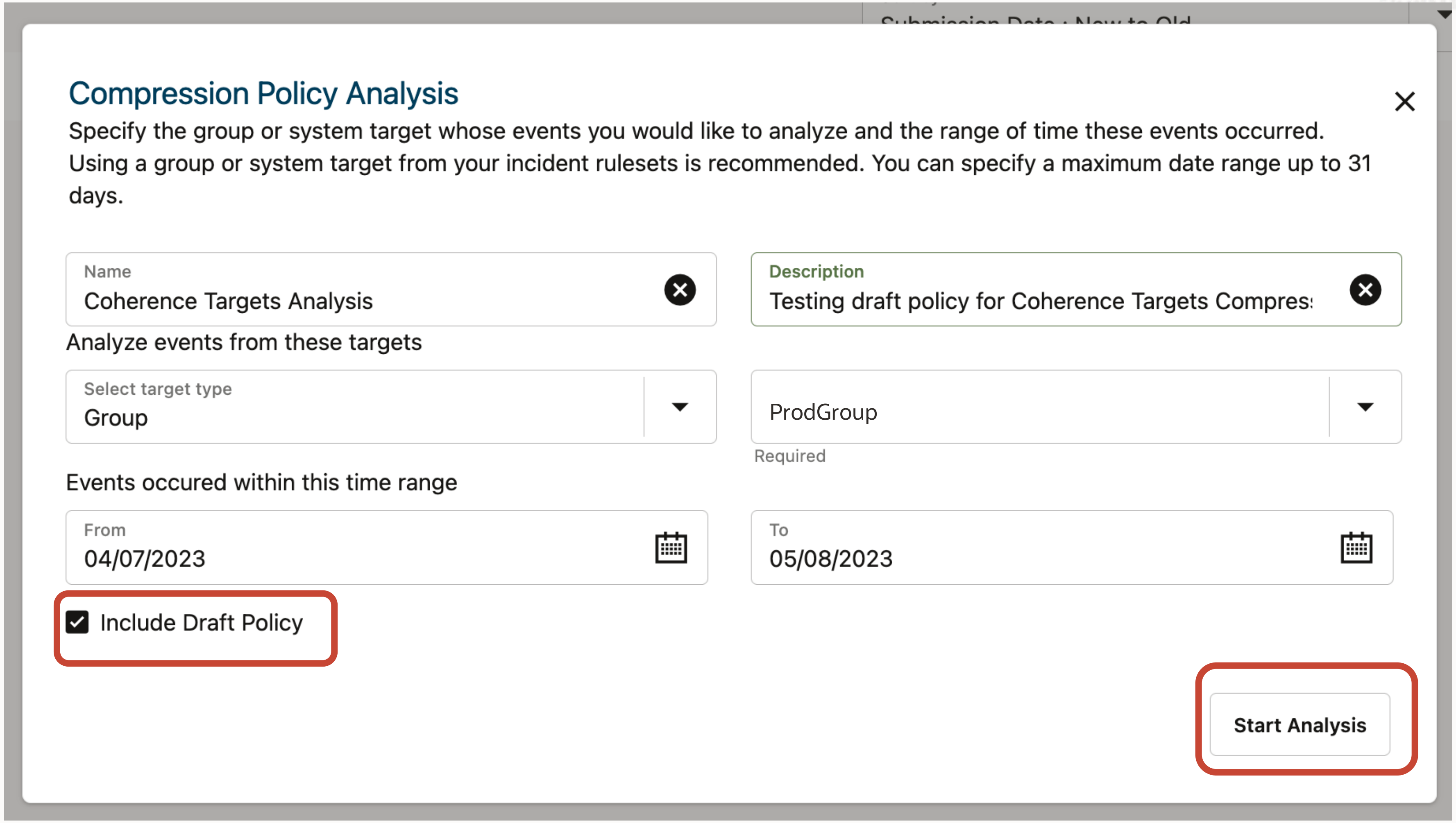
Completed
Submitted on Apr 16, 2023 8:14:28 PM PDT
View Job Details

Events From Database System Oemrep_Database_sys
From Mar 16, 2023 12:00:00 AM PDT
To Apr 16, 2023 11:59:59 PM PDT

Description

Event Compression Analysis

Start analysis



Compression Policy Analysis

Specify the group or system target whose events you would like to analyze and the range of time these events occurred. Using a group or system target from your incident rulesets is recommended. You can specify a maximum date range up to 31 days.

Name: Coherence Targets Analysis

Description: Testing draft policy for Coherence Targets Compres:

Analyze events from these targets

Select target type: Group

ProdGroup

Required

Events occured within this time range

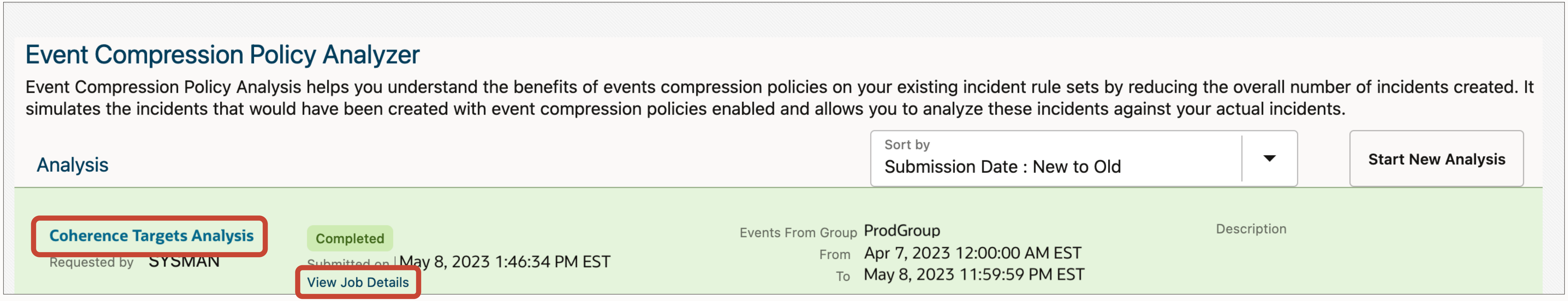
From: 04/07/2023

To: 05/08/2023

☑ Include Draft Policy

Event Compression Analysis

Policy analysis job…Start → In-Progress → Completed



Event Compression Policy Analyzer

Event Compression Policy Analysis helps you understand the benefits of events compression policies on your existing incident rule sets by reducing the overall number of incidents created. It simulates the incidents that would have been created with event compression policies enabled and allows you to analyze these incidents against your actual incidents.

Analysis

Sort by: Submission Date : New to Old

Coherence Targets Analysis

Requested by SYSMAN

Completed

Submitted on May 8, 2023 1:46:34 PM EST

Events From Group ProdGroup

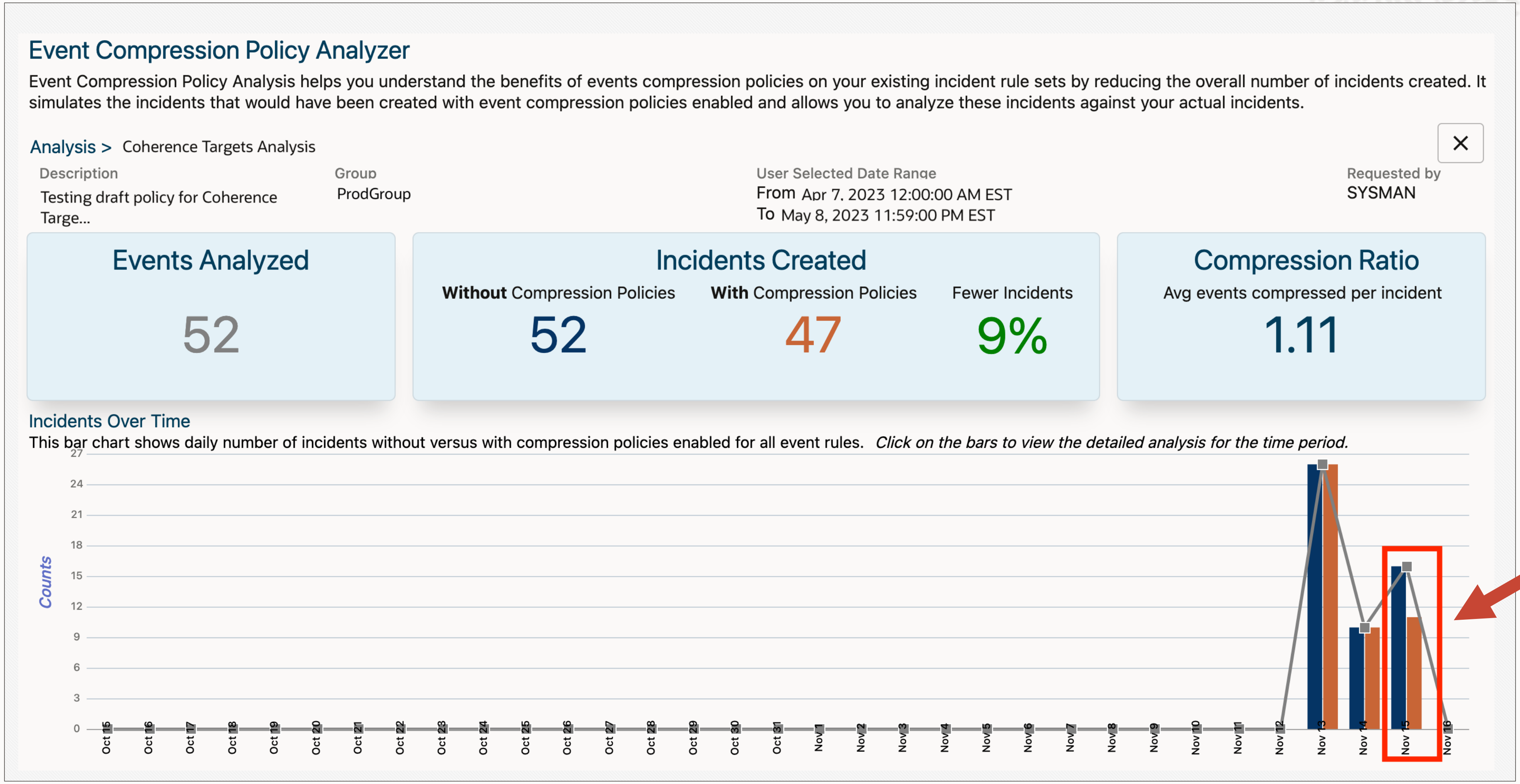
From Apr 7, 2023 12:00:00 AM EST

To May 8, 2023 11:59:59 PM EST

Description

Event Compression Analysis

Analysis results pt.1



Event Compression Policy Analyzer

Event Compression Policy Analysis helps you understand the benefits of events compression policies on your existing incident rule sets by reducing the overall number of incidents created. It simulates the incidents that would have been created with event compression policies enabled and allows you to analyze these incidents against your actual incidents.

Analysis > Coherence Targets Analysis

Description	Group	User Selected Date Range	Requested by
Testing draft policy for Coherence Targe...	ProdGroup	From Apr 7, 2023 12:00:00 AM EST To May 8, 2023 11:59:00 PM EST	SYSMAN

Events Analyzed

52

Incidents Created

Without Compression Policies	**With** Compression Policies	Fewer Incidents
52	47	9%

Compression Ratio

Avg events compressed per incident

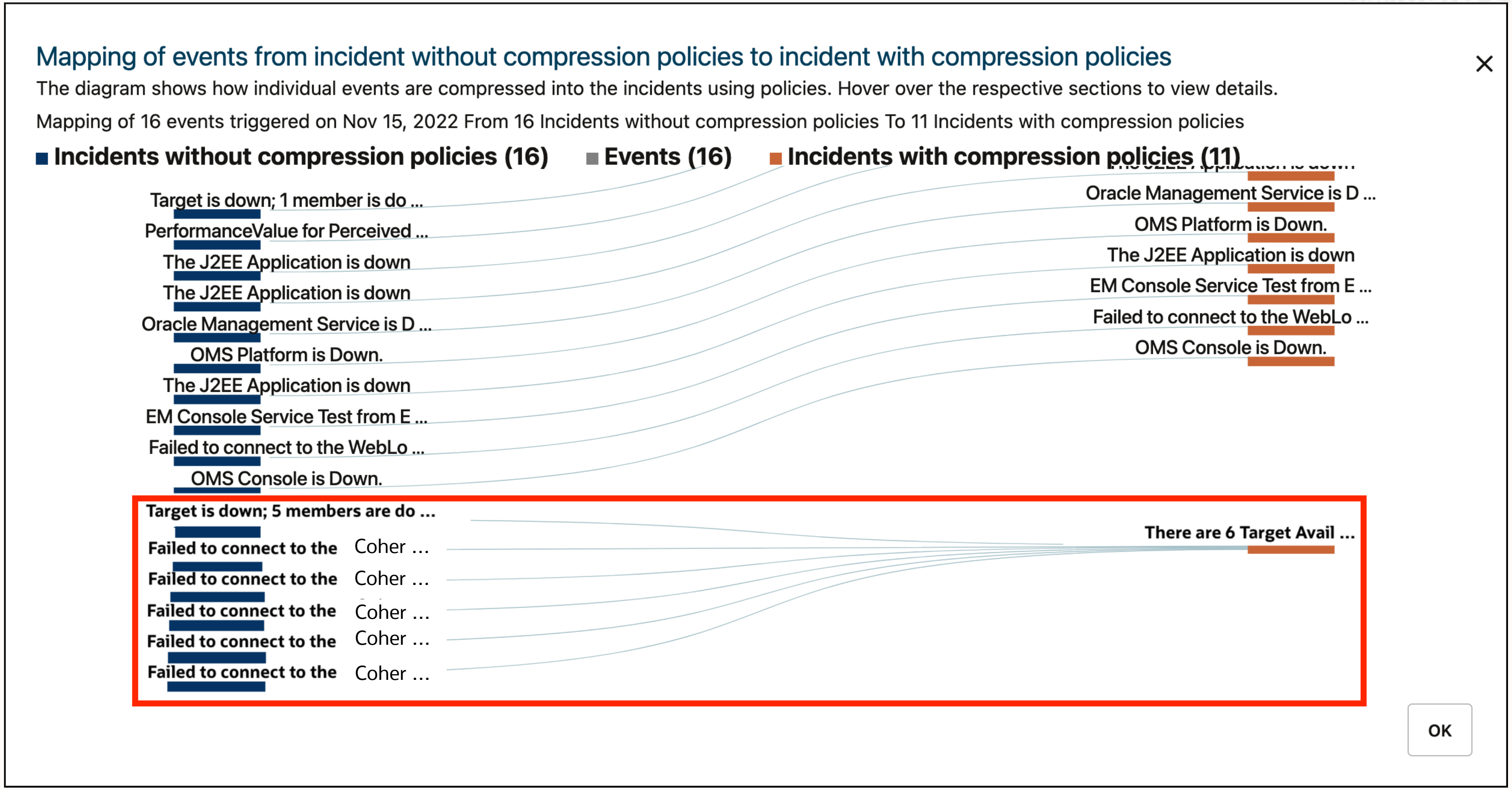
1.11

Incidents Over Time

This bar chart shows daily number of incidents without versus with compression policies enabled for all event rules. *Click on the bars to view the detailed analysis for the time period.*

Event Compression Analysis

Analysis results pt.2



Mapping of events from incident without compression policies to incident with compression policies

The diagram shows how individual events are compressed into the incidents using policies. Hover over the respective sections to view details.

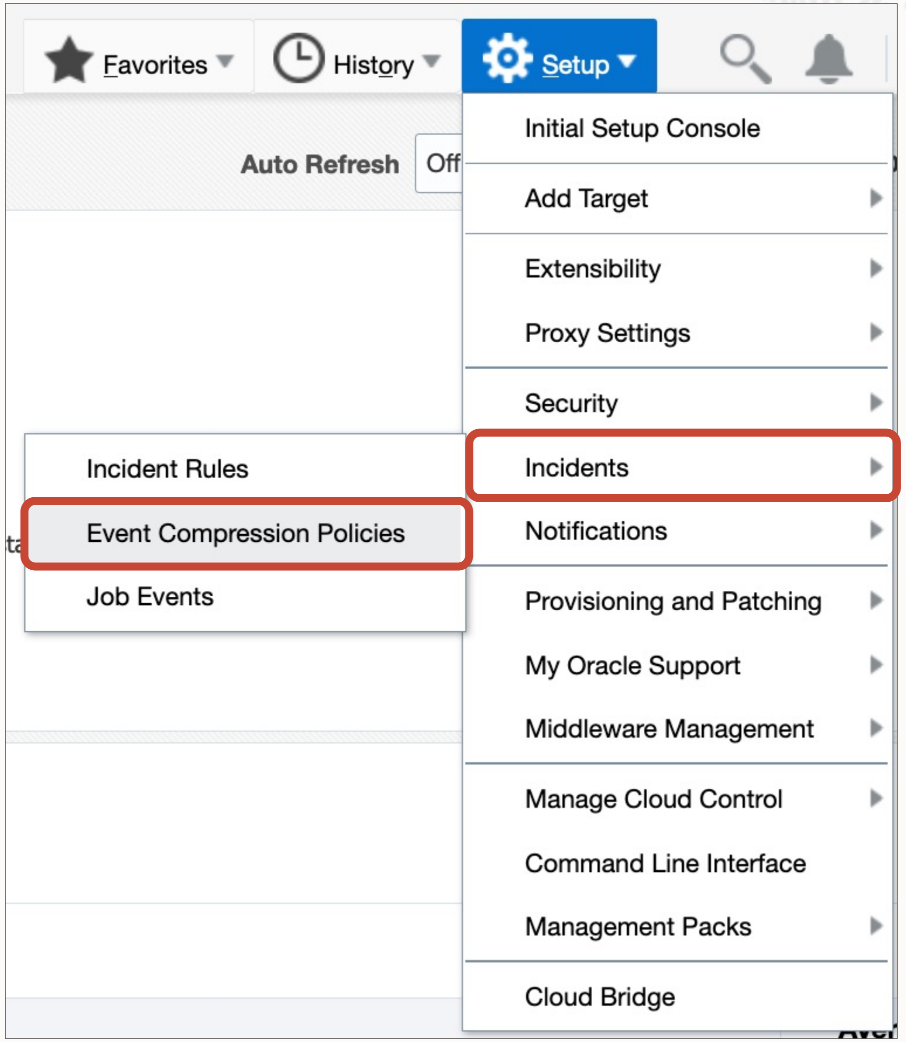
Mapping of 16 events triggered on Nov 15, 2022 From 16 Incidents without compression policies To 11 Incidents with compression policies

■ Incidents without compression policies (16)
■ Events (16)
■ Incidents with compression policies (11)
Target is down; 1 member is do ...
PerformanceValue for Perceived ...
The J2EE Application is down
The J2EE Application is down
Oracle Management Service is D ...
OMS Platform is Down.
The J2EE Application is down
EM Console Service Test from E ...
Failed to connect to the WebLo ...
OMS Console is Down.
Target is down; 5 members are do ...
Failed to connect to the Coher ...
Failed to connect to the Coher ...
Failed to connect to the Coher ...
Failed to connect to the Coher ...
Failed to connect to the Coher ...
Oracle Management Service is D ...
OMS Platform is Down.
The J2EE Application is down
EM Console Service Test from E ...
Failed to connect to the WebLo ...
OMS Console is Down.
There are 6 Target Avail ...
×
OK

User-Defined Policies

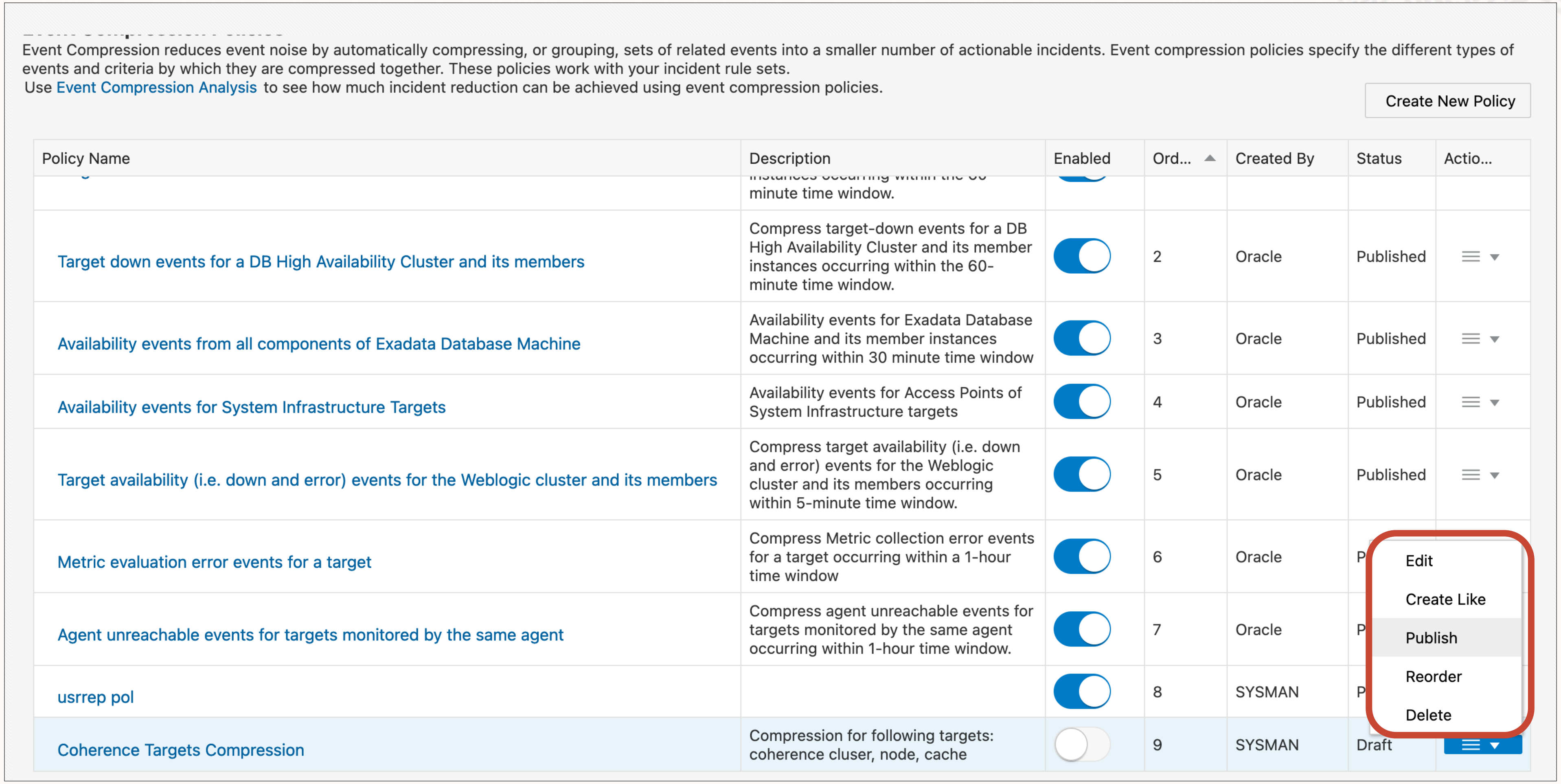
Navigating to Event Compression Policies

Setup > Incidents > Event Compression Policies



User-Defined Policies

Event Compression Policy actions



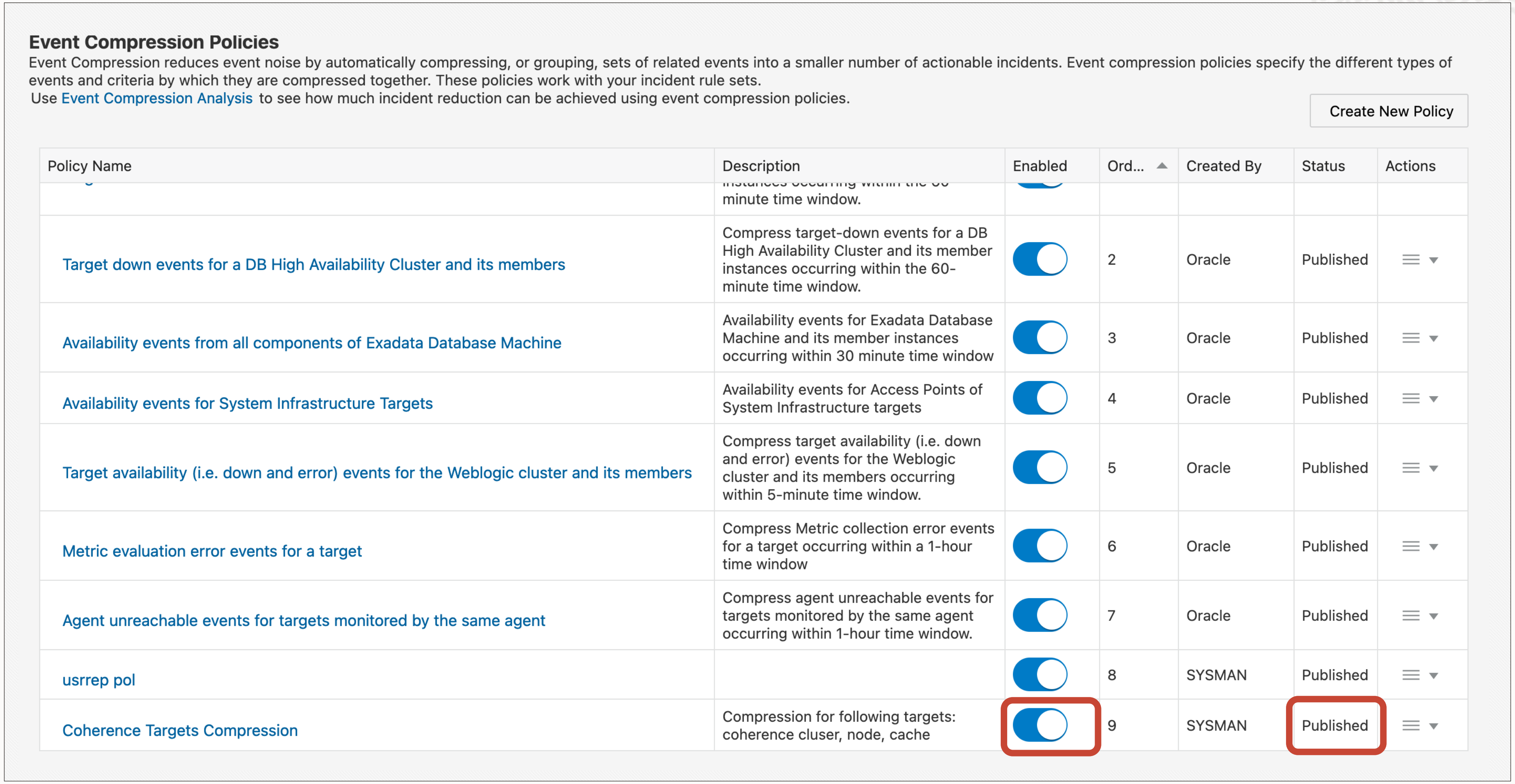
Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Policy Name	Description	Enabled	Ord...	Created By	Status	Actio...
	minute time window.	●				
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	≡ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	≡ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	≡ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	≡ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	P	
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	P	
usrrep pol		●	8	SYSMAN	P	
Coherence Targets Compression	Compression for following targets: coherence cluser, node, cache	○	9	SYSMAN	Draft	≡ ▾

User-Defined Policies

Publish and enable the policy



Event Compression Policies

Event Compression reduces event noise by automatically compressing, or grouping, sets of related events into a smaller number of actionable incidents. Event compression policies specify the different types of events and criteria by which they are compressed together. These policies work with your incident rule sets.

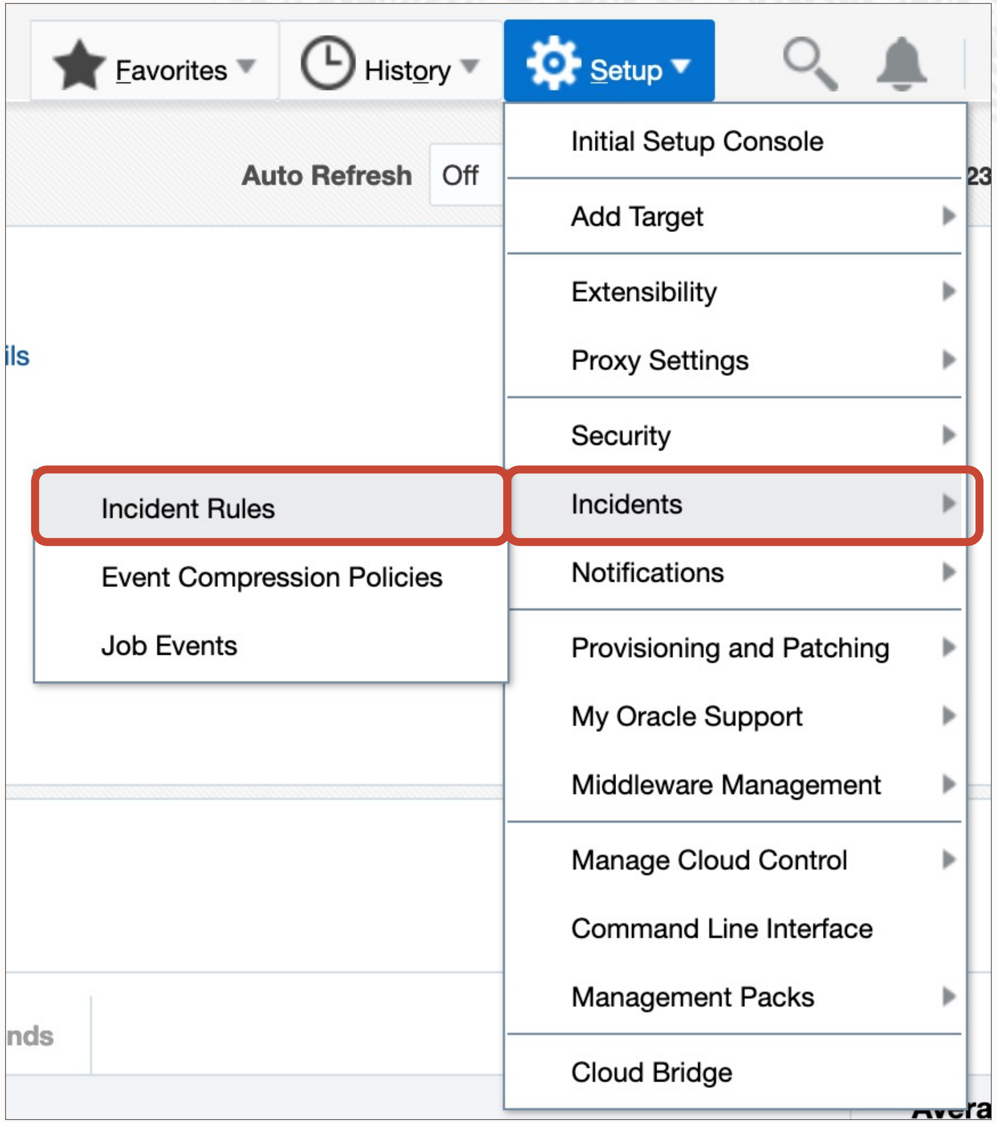
Use Event Compression Analysis to see how much incident reduction can be achieved using event compression policies.

Policy Name	Description	Enabled	Ord... ▲	Created By	Status	Actions
	minute time window.	●				
Target down events for a DB High Availability Cluster and its members	Compress target-down events for a DB High Availability Cluster and its member instances occurring within the 60-minute time window.	●	2	Oracle	Published	☰ ▾
Availability events from all components of Exadata Database Machine	Availability events for Exadata Database Machine and its member instances occurring within 30 minute time window	●	3	Oracle	Published	☰ ▾
Availability events for System Infrastructure Targets	Availability events for Access Points of System Infrastructure targets	●	4	Oracle	Published	☰ ▾
Target availability (i.e. down and error) events for the Weblogic cluster and its members	Compress target availability (i.e. down and error) events for the Weblogic cluster and its members occurring within 5-minute time window.	●	5	Oracle	Published	☰ ▾
Metric evaluation error events for a target	Compress Metric collection error events for a target occurring within a 1-hour time window	●	6	Oracle	Published	☰ ▾
Agent unreachable events for targets monitored by the same agent	Compress agent unreachable events for targets monitored by the same agent occurring within 1-hour time window.	●	7	Oracle	Published	☰ ▾
usrrep pol		●	8	SYSMAN	Published	☰ ▾
Coherence Targets Compression	Compression for following targets: coherence cluser, node, cache	●	9	SYSMAN	Published	☰ ▾

User-Defined Policies

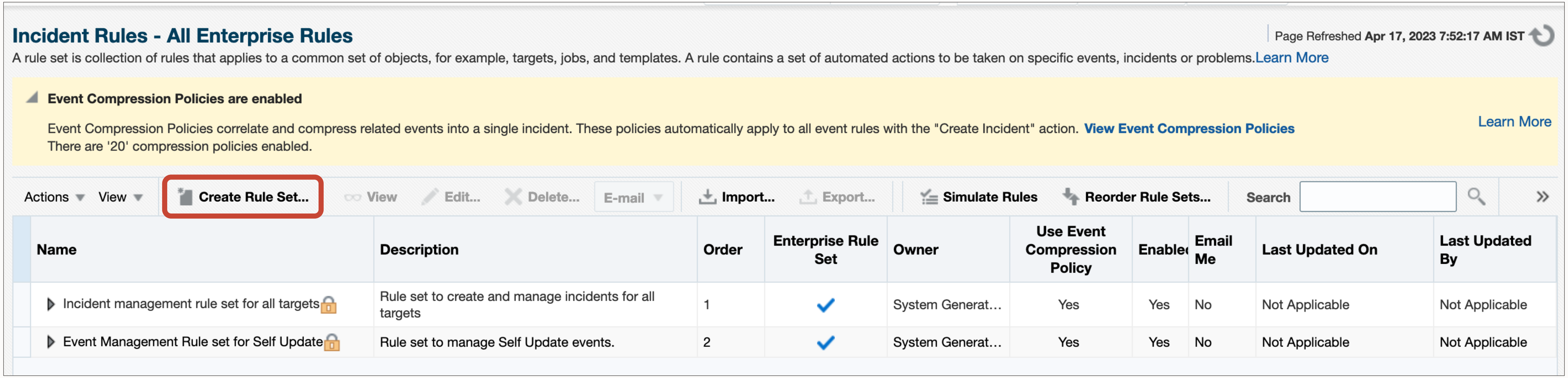
Navigating to Incident Rules

Setup > Incident > Incident Rules



User-Defined Policies

Incident Rules - Create Rule Set



Incident Rules - All Enterprise Rules

Page Refreshed **Apr 17, 2023 7:52:17 AM IST**

A rule set is collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems.Learn More

Event Compression Policies are enabled

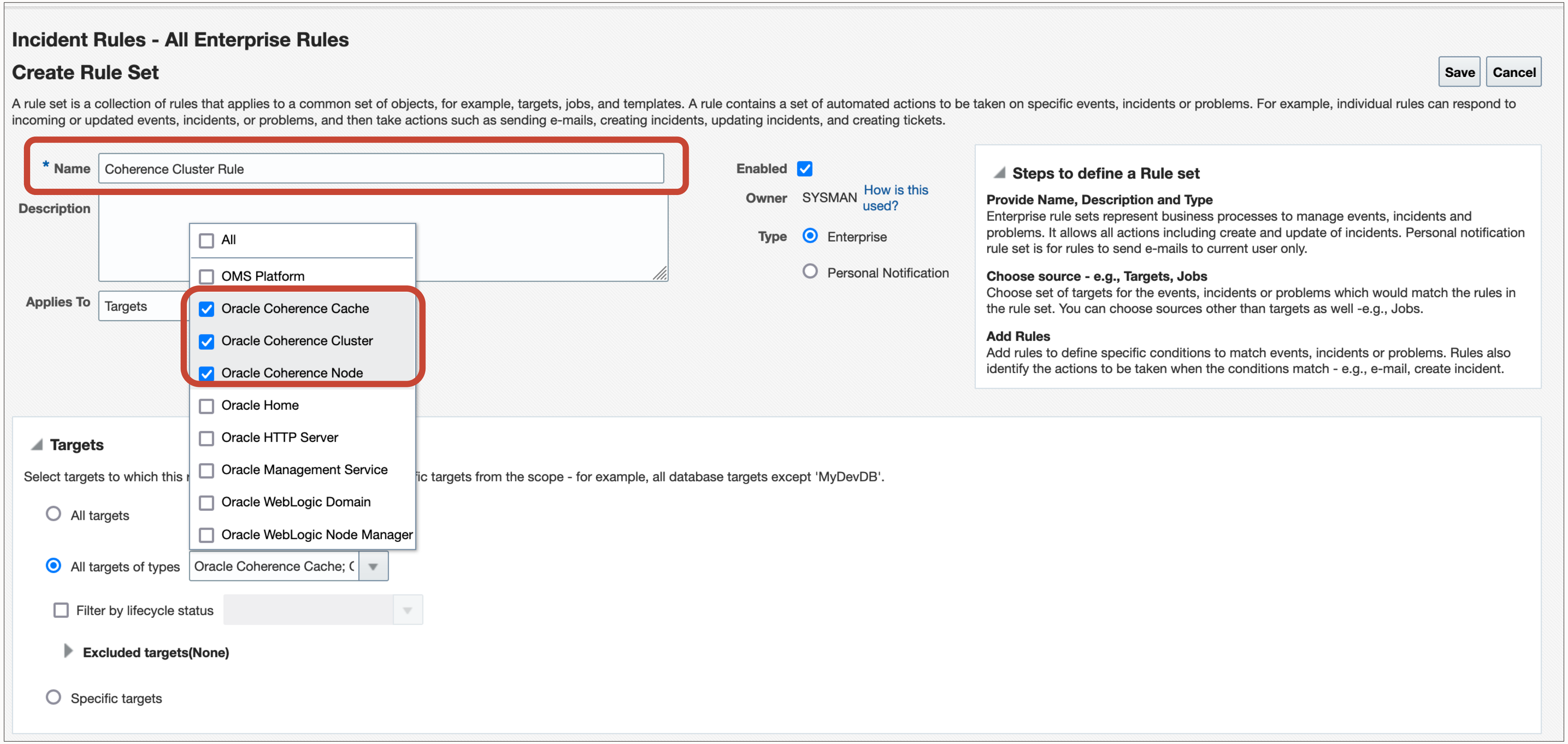
Event Compression Policies correlate and compress related events into a single incident. These policies automatically apply to all event rules with the "Create Incident" action. **View Event Compression Policies** Learn More

There are '20' compression policies enabled.

Name	Description	Order	Enterprise Rule Set	Owner	Use Event Compression Policy	Enablec	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat…	Yes	Yes	No	Not Applicable	Not Applicable
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat…	Yes	Yes	No	Not Applicable	Not Applicable

User-Defined Policies

Incident Rules - Specify the name of rule set and select targets to apply on



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: Coherence Cluster Rule

Description:

Applies To: Targets

- □ All
- □ OMS Platform
- ☑ Oracle Coherence Cache
- ☑ Oracle Coherence Cluster
- ☑ Oracle Coherence Node
- □ Oracle Home
- □ Oracle HTTP Server
- □ Oracle Management Service
- □ Oracle WebLogic Domain
- □ Oracle WebLogic Node Manager

Enabled ☑

Owner: SYSMAN How is this used?

Type: ● Enterprise ○ Personal Notification

Steps to define a Rule set

Provide Name, Description and Type
Enterprise rule sets represent business processes to manage events, incidents and problems. It allows all actions including create and update of incidents. Personal notification rule set is for rules to send e-mails to current user only.

Choose source - e.g., Targets, Jobs
Choose set of targets for the events, incidents or problems which would match the rules in the rule set. You can choose sources other than targets as well -e.g., Jobs.

Add Rules
Add rules to define specific conditions to match events, incidents or problems. Rules also identify the actions to be taken when the conditions match - e.g., e-mail, create incident.

Targets

Select targets to which this r ic targets from the scope - for example, all database targets except 'MyDevDB'.

○ All targets

● All targets of types: Oracle Coherence Cache; (

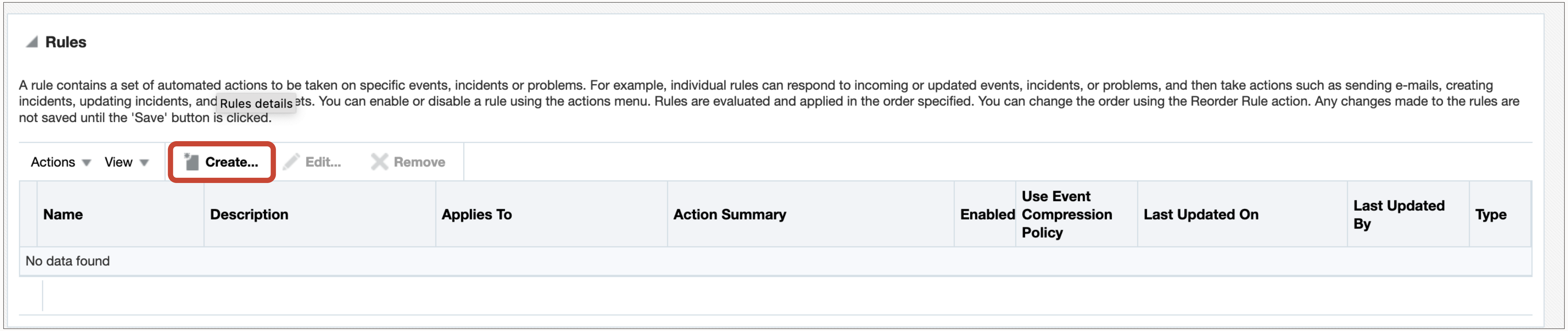
□ Filter by lifecycle status

Excluded targets(None)

○ Specific targets

User-Defined Policies

Incident Rules – Create rule



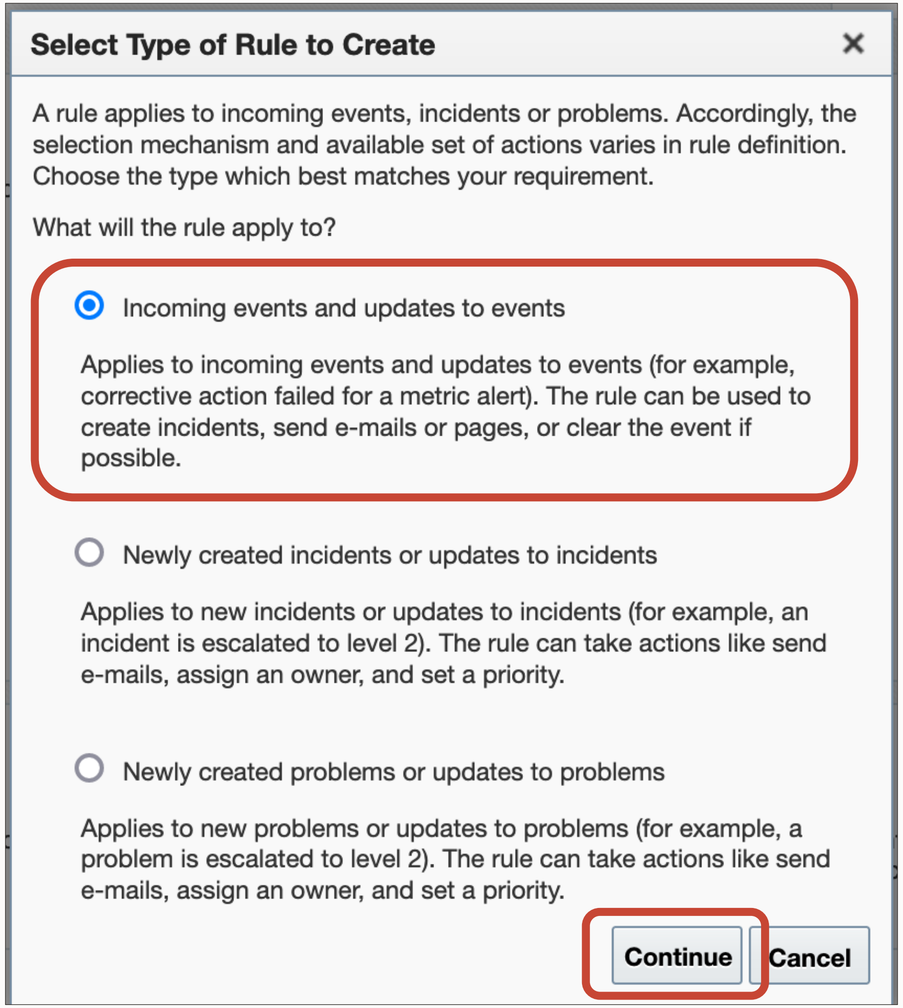
Rules

A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and Rules details ets. You can enable or disable a rule using the actions menu. Rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule action. Any changes made to the rules are not saved until the 'Save' button is clicked.

Name	Description	Applies To	Action Summary	Enabled	Use Event Compression Policy	Last Updated On	Last Updated By	Type
No data found								

User-Defined Policies

Incident Rules – Select for incoming events



Select Type of Rule to Create ✕

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

What will the rule apply to?

● Incoming events and updates to events

Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

○ Newly created incidents or updates to incidents

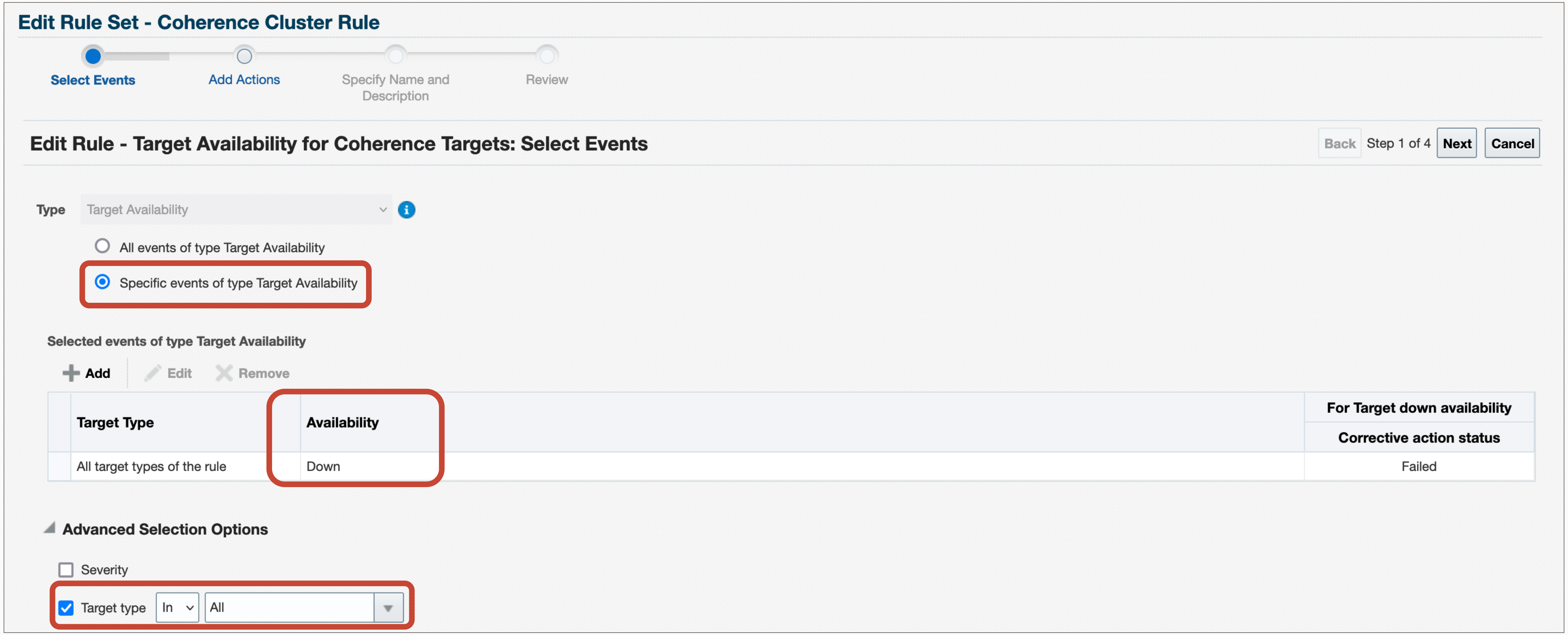
Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

○ Newly created problems or updates to problems

Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

User-Defined Policies

Incident Rules – Select event criteria



Edit Rule Set - Coherence Cluster Rule

Edit Rule - Target Availability for Coherence Targets: Select Events

Type: Target Availability

○ All events of type Target Availability

● Specific events of type Target Availability

Selected events of type Target Availability

Target Type	Availability	For Target down availability Corrective action status
All target types of the rule	Down	Failed

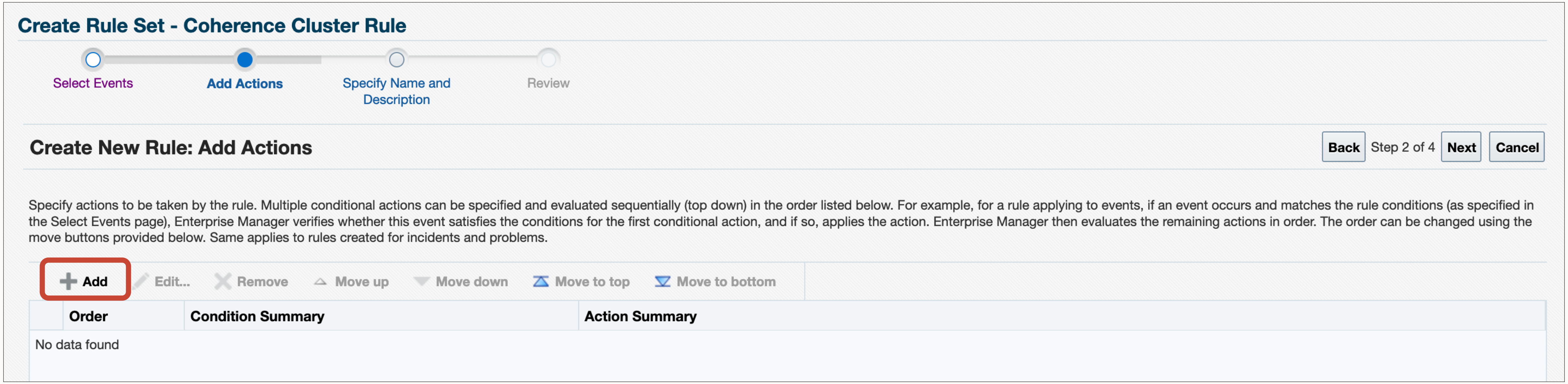
Advanced Selection Options

□ Severity

☑ Target type In All

User-Defined Policies

Incident Rules - Add actions



Create Rule Set - Coherence Cluster Rule

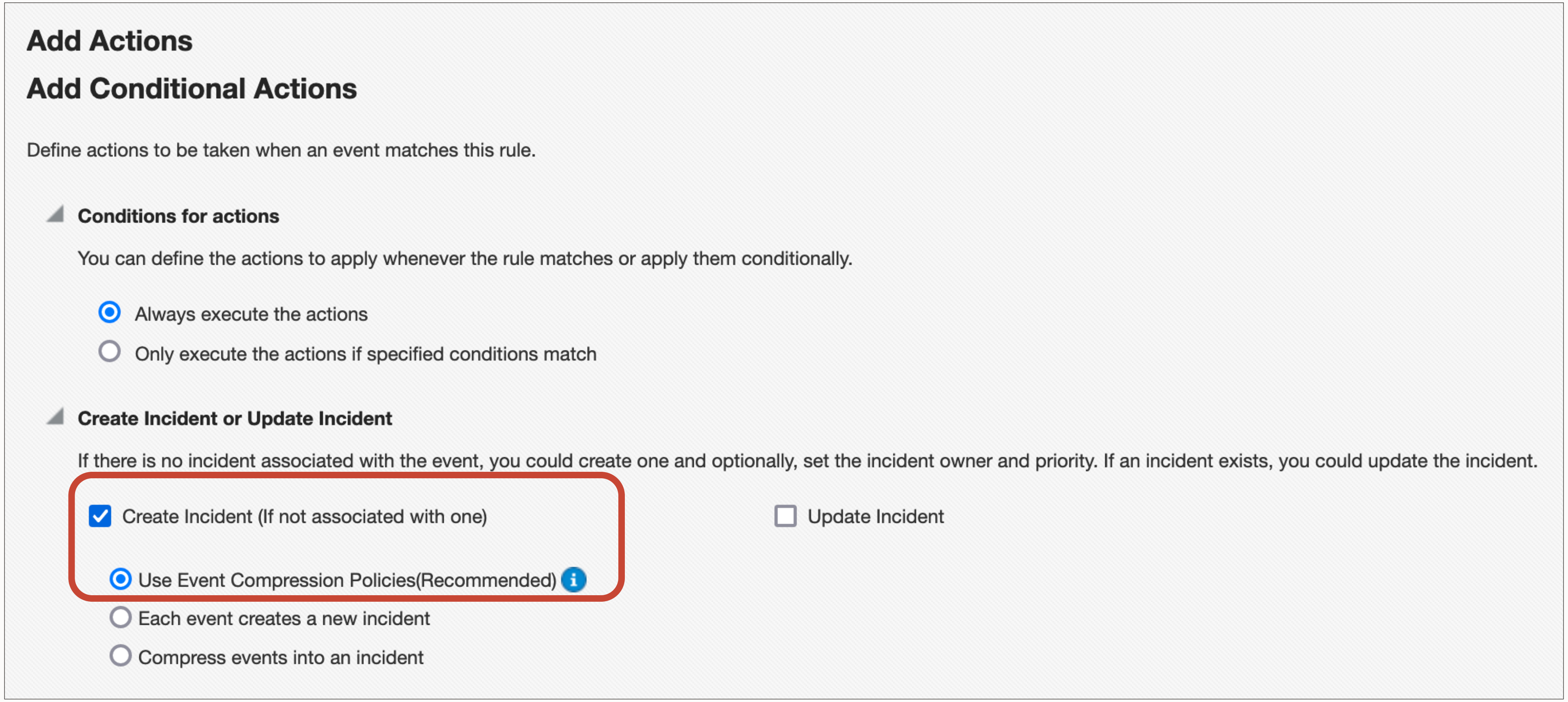
Create New Rule: Add Actions

Specify actions to be taken by the rule. Multiple conditional actions can be specified and evaluated sequentially (top down) in the order listed below. For example, for a rule applying to events, if an event occurs and matches the rule conditions (as specified in the Select Events page), Enterprise Manager verifies whether this event satisfies the conditions for the first conditional action, and if so, applies the action. Enterprise Manager then evaluates the remaining actions in order. The order can be changed using the move buttons provided below. Same applies to rules created for incidents and problems.

Order	Condition Summary	Action Summary
No data found		

User-Defined Policies

Incident Rules – Add conditions for actions



Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

● Always execute the actions

○ Only execute the actions if specified conditions match

Create Incident or Update Incident

If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

☑ Create Incident (If not associated with one)

□ Update Incident

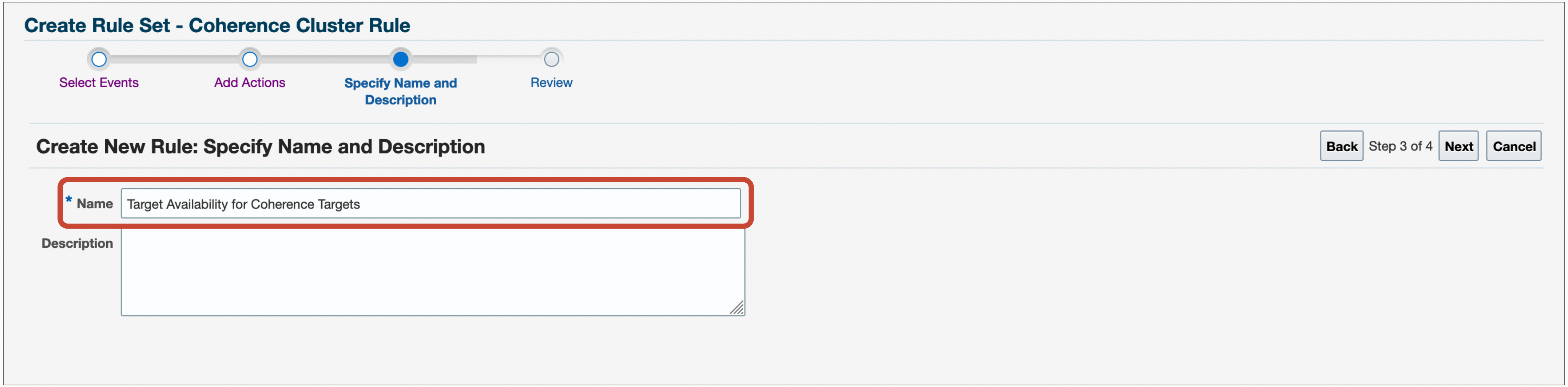
● Use Event Compression Policies(Recommended)

○ Each event creates a new incident

○ Compress events into an incident

User-Defined Policies

Incident Rules – Specify name and description



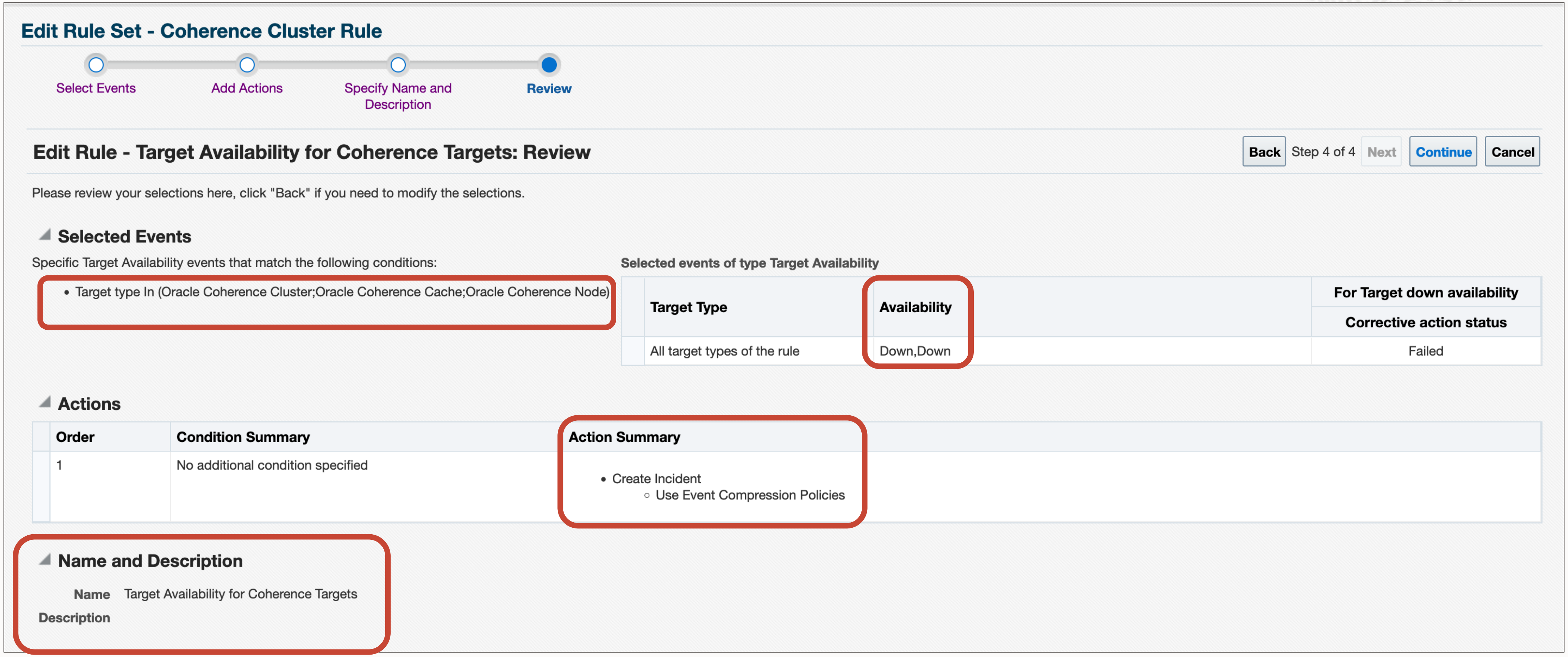
Create Rule Set - Coherence Cluster Rule
Select Events
Add Actions
Specify Name and Description
Review
Back
Step 3 of 4
Next
Cancel

Create New Rule: Specify Name and Description

* Name	Target Availability for Coherence Targets
Description	

User-Defined Policies

Incident Rules – Review rule created



Edit Rule Set - Coherence Cluster Rule
Select Events
Add Actions
Specify Name and Description
Review
Back
Step 4 of 4
Next
Continue
Cancel

Edit Rule - Target Availability for Coherence Targets: Review

Please review your selections here, click "Back" if you need to modify the selections.

Selected Events

Specific Target Availability events that match the following conditions:

- Target type In (Oracle Coherence Cluster;Oracle Coherence Cache;Oracle Coherence Node)

Selected events of type Target Availability

Target Type	Availability	For Target down availability Corrective action status
All target types of the rule	Down,Down	Failed

Actions

Order	Condition Summary	Action Summary
1	No additional condition specified	• Create Incident ○ Use Event Compression Policies

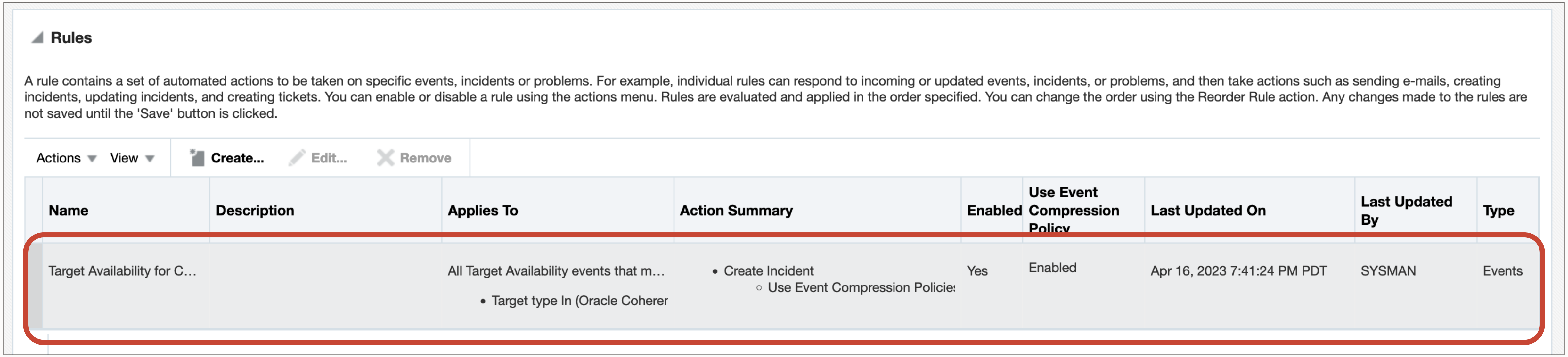
Name and Description

Name Target Availability for Coherence Targets

Description

User-Defined Policies

Incident Rules – Rule created

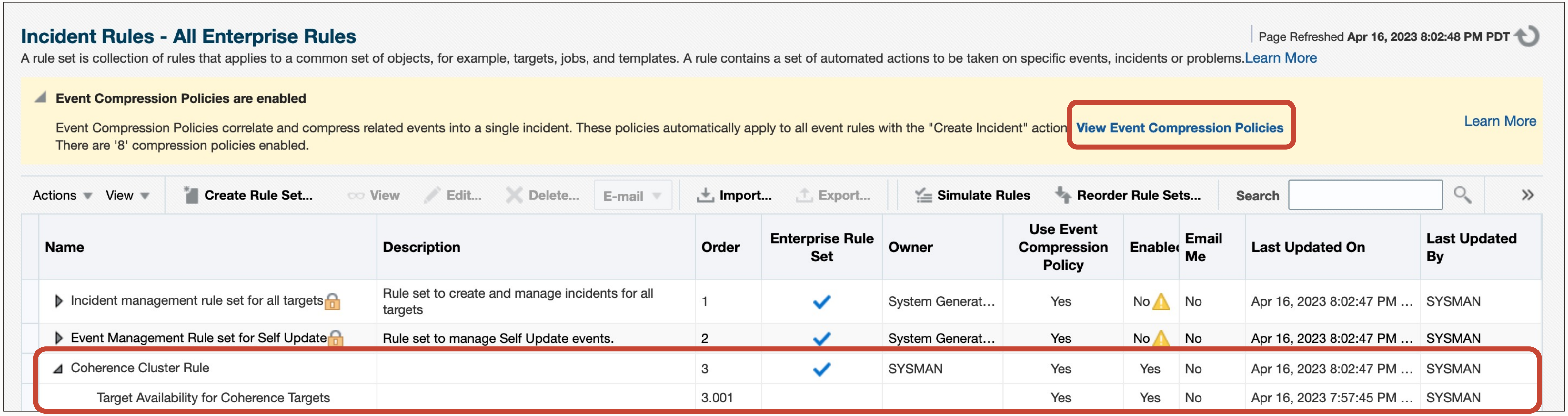


A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. You can enable or disable a rule using the actions menu. Rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule action. Any changes made to the rules are not saved until the 'Save' button is clicked.

Name	Description	Applies To	Action Summary	Enabled	Use Event Compression Policy	Last Updated On	Last Updated By	Type
Target Availability for C…		All Target Availability events that m… • Target type In (Oracle Coherer	• Create Incident ○ Use Event Compression Policie:	Yes	Enabled	Apr 16, 2023 7:41:24 PM PDT	SYSMAN	Events

User-Defined Policies

Incident Rules – Rule saved



Incident Rules - All Enterprise Rules

Page Refreshed **Apr 16, 2023 8:02:48 PM PDT**

A rule set is collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems.Learn More

Event Compression Policies are enabled

Event Compression Policies correlate and compress related events into a single incident. These policies automatically apply to all event rules with the "Create Incident" action **View Event Compression Policies** Learn More
There are '8' compression policies enabled.

Name	Description	Order	Enterprise Rule Set	Owner	Use Event Compression Policy	Enabled	Email Me	Last Updated On	Last Updated By
▸ Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat...	Yes	No ⚠	No	Apr 16, 2023 8:02:47 PM ...	SYSMAN
▸ Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat...	Yes	No ⚠	No	Apr 16, 2023 8:02:47 PM ...	SYSMAN
◢ Coherence Cluster Rule		3	✓	SYSMAN	Yes	Yes	No	Apr 16, 2023 8:02:47 PM ...	SYSMAN
Target Availability for Coherence Targets		3.001			Yes	Yes	No	Apr 16, 2023 7:57:45 PM ...	SYSMAN

Rule enabled to begin compression of Coherence targets per the user-defined policy

Reducing event noise with Event Compression

- Event Compression groups related events into a smaller set of actionable incidents to reduce event noise
  - Two types:
    - Event Compression Policies (recommended)
    - Rule-Based Event Compression
- Oracle provides seven OOB policies
- Can create your own policies
- Use the Event Compression Analysis tool to test out your policy before publishing and enabling it for use

Resources

1. Event Compression Policies Documentation
2. Videohub: Manage Incidents More Effectively with Event Compression and Dynamic Runbooks
3. Blog: Reducing alert fatigue with Event Compression Policies in Oracle Enterprise Manager
4. Other Related Blogs

Thank You!

Contact: desiree.abrokwa@oracle.com

ORACLE