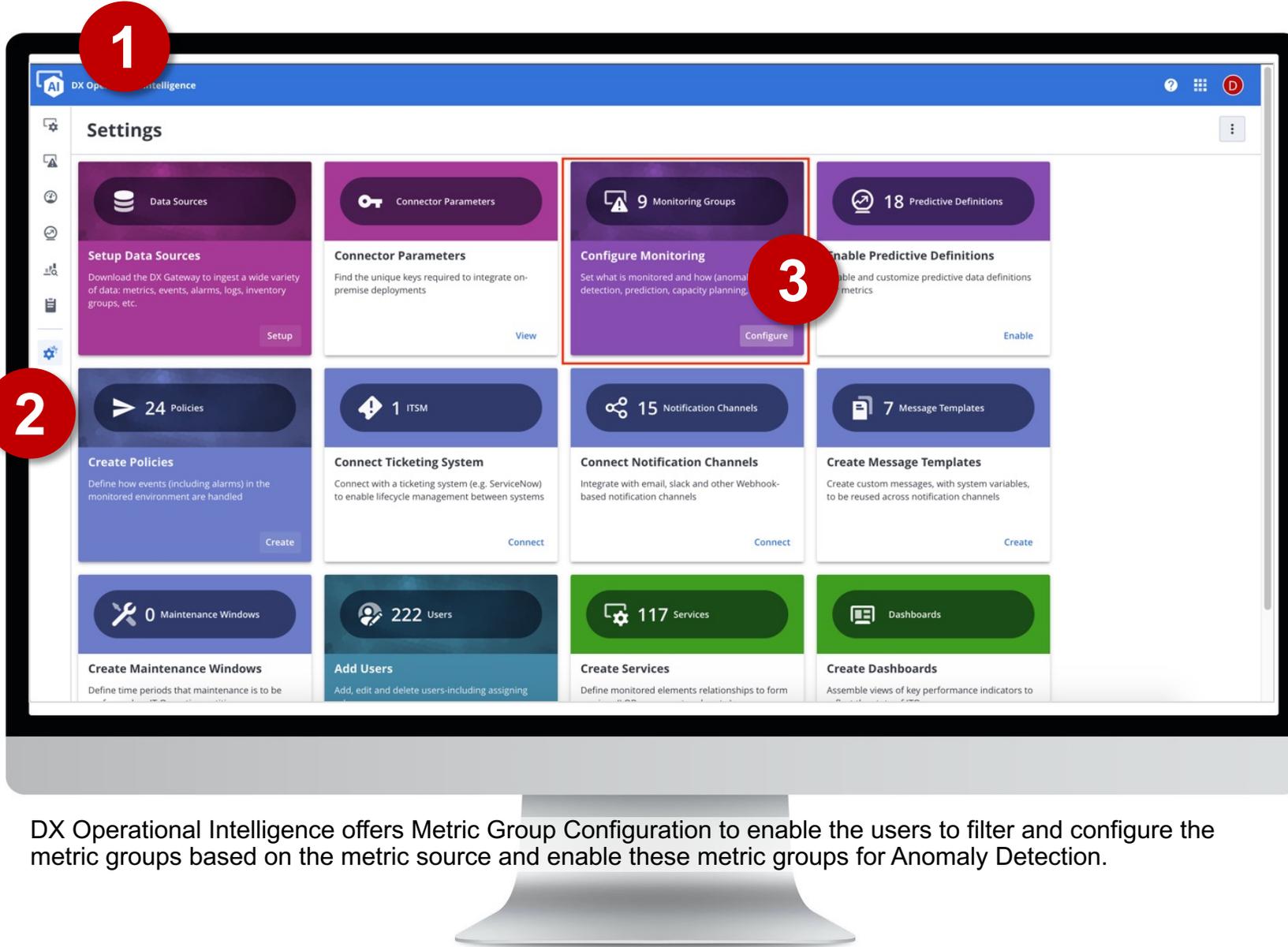


Product Tutorial

DX Operational Intelligence

Configuring Anomaly Detection

Configuring Metric Groups For Anomaly Detection #1



1. Launch DX Operational Intelligence
2. Click on “Settings” in the left navigation menu
3. Click “Configure” on the “Monitoring Groups” card

DX Operational Intelligence offers Metric Group Configuration to enable the users to filter and configure the metric groups based on the metric source and enable these metric groups for Anomaly Detection.

Configuring Metric Groups For Anomaly Detection #2

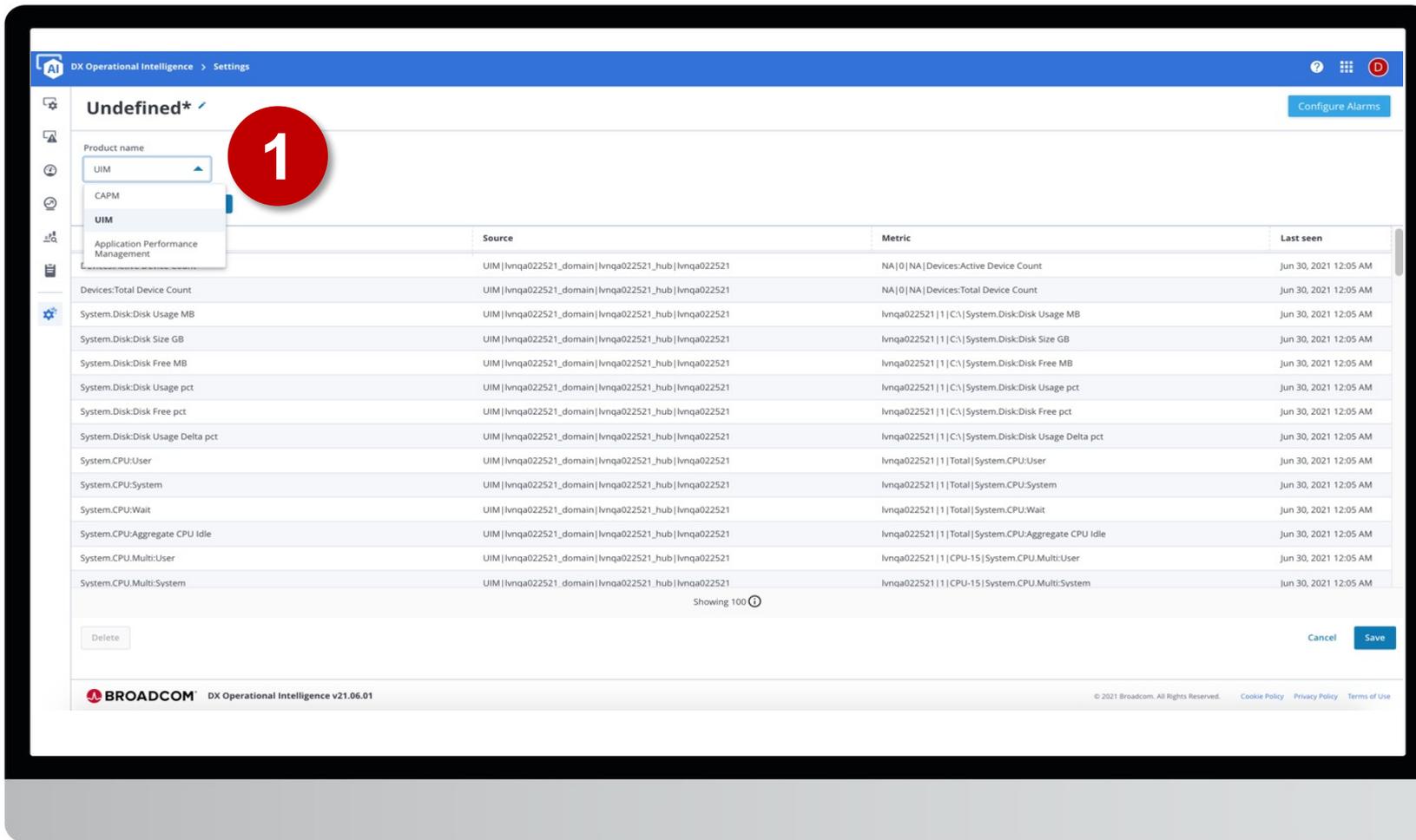
The screenshot displays the 'Metric Monitoring Groups' configuration page in the DX Operational Intelligence interface. The page shows a table of metric groups with columns for Group name, Description, Filters, Product, Anomaly detection, and Last editor. A red circle with the number '2' is positioned in the top right corner of the interface, pointing to the '+ Create metric monitoring group' button. Another red circle with the number '1' is positioned in the bottom right corner of the table area, pointing to the 'Anomaly detection' toggle for the 'Test1' group.

Group name	Description	Filters	Product	Anomaly detection	Last editor
<input type="checkbox"/> APM Avg Reponse Time (168)		Metric: Response Time (ms)(ends_with)	Application Performance Mana...	<input type="checkbox"/>	NESTOR.FALCO...
<input type="checkbox"/> APM - Frontends metrics and c... (30)		Metric: (Frontends\ Apps\[^\]* CPU\ Processor.* CPU.* GC Monitor....	Application Performance Mana...	<input checked="" type="checkbox"/>	NESTOR.FALCO...
<input type="checkbox"/> CAPM - all utilizations via reg... (1247)		Metric: *(applicationCPUUtilization cpuSystemUtilization heapUtilizati...	CAPM	<input checked="" type="checkbox"/>	NESTOR.FALCO...
<input type="checkbox"/> CAPM - cpu and interface util... (1263)		Metric: Utilization(contains)	CAPM	<input checked="" type="checkbox"/>	NESTOR.FALCO...
<input type="checkbox"/> Core Network Metrics (36)		Metric: reach(contains)	CAPM	<input type="checkbox"/>	FRANCOIS.CATT...
<input type="checkbox"/> Default 3rd Party Metric Group (0)	A default list of 3rd party integrated...	Source: custom\ .*(regex)	CUSTOM	<input type="checkbox"/>	DEFAULTORG
<input type="checkbox"/> Test1 (651)	test	Metric: CPU(contains)	UIM	<input type="checkbox"/>	NESTOR.FALCO...
<input type="checkbox"/> UIM CPU Usage (135)		Metric: CPU Usage(ends_with)	UIM	<input checked="" type="checkbox"/>	NESTOR.FALCO...
<input type="checkbox"/> UIM Memory Usage (68)		Metric: Memory Usage pct(contains)	UIM	<input checked="" type="checkbox"/>	NESTOR.FALCO...

1. Toggle anomaly detection on/off if you want to change activation status for an existing groups
2. Click on the “+ Create metric monitoring group” button placed on the right-hand top corner if you want to create a new group of metrics

This screen lists the metric group name, its description provided during the creation, the filters used to create the metric group, a toggle to Anomaly Detection on/off for the group, the metric source and the last editor of the metric group configuration.

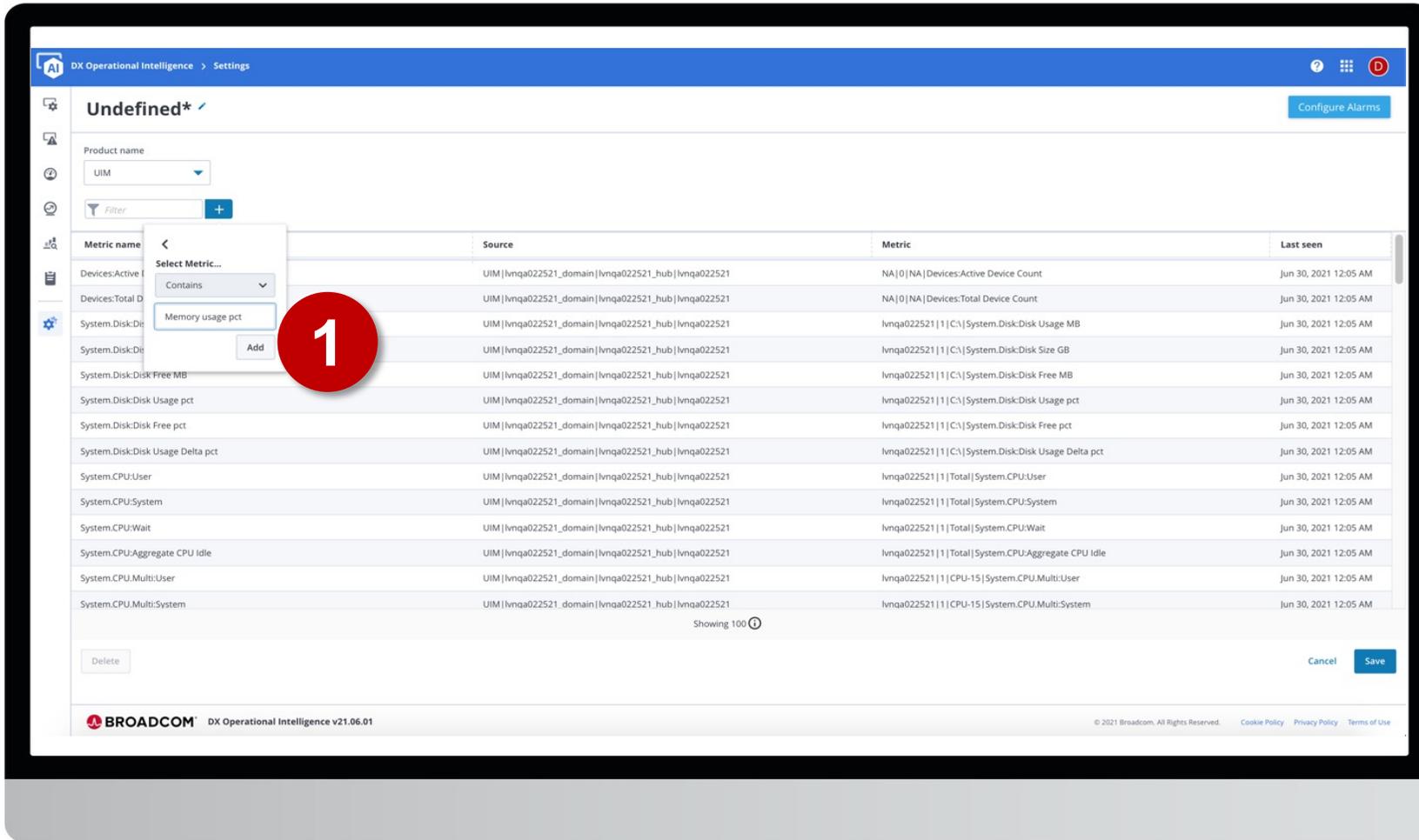
Configuring Metric Groups for Anomaly Detection #3



1. Select the product from which you get the metrics

To create the metric monitoring group, you have to first select the source product for the metrics from the drop down. This dropdown will contain all the source products for which the metrics are present in the DX Operational Intelligence repository.

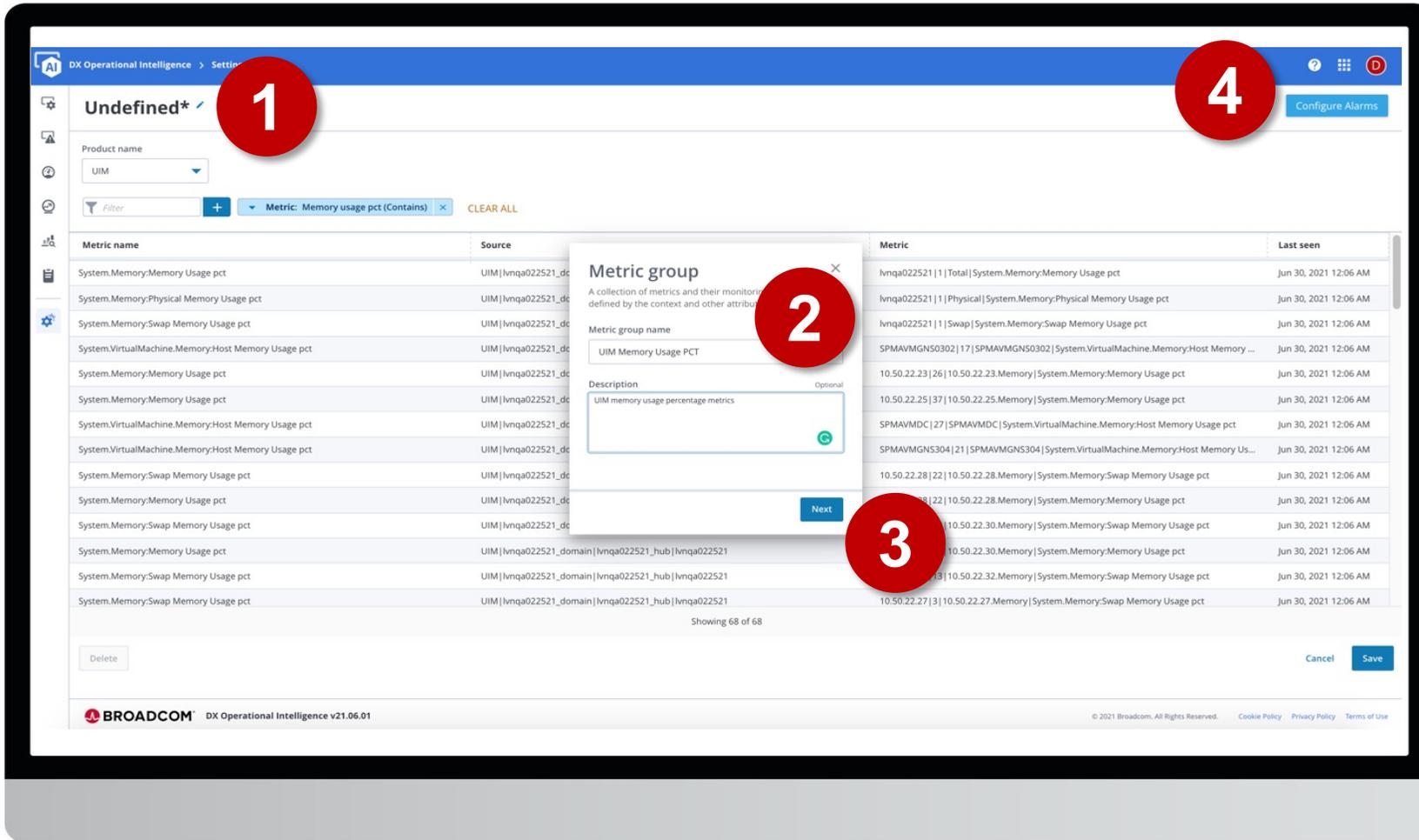
Configuring Metric Groups For Anomaly Detection #4



1. Set a relevant filter for the metrics to be used in the group

Use the filter to select metric names or the device sources. In this screen, the filter is set on the Metric name and looking for only for the metric names containing "Memory usage pct".

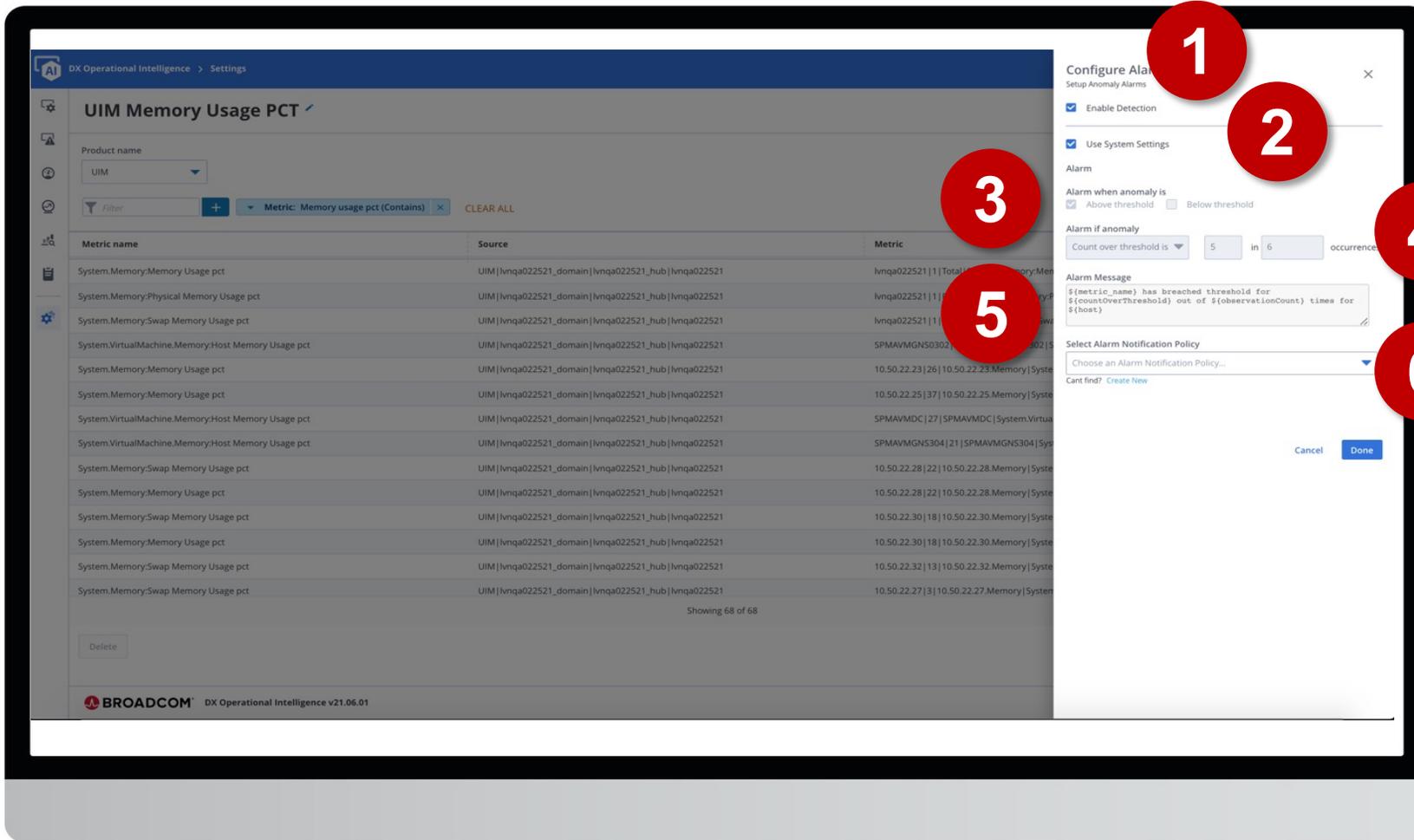
Configuring Metric Groups For Anomaly Detection #5



1. Click on the “edit” icon next to the “Undefined*” text on top of the screen
2. Give a name and description to the metric monitoring group in the dialog panel
3. Click on “Next” to save your changes
4. Click on the “Configure Alarm” if you need to fine tune anomaly alarms

Give a name and description to the metric monitoring group, this name and description will be displayed on the Metric Monitoring Group screen.

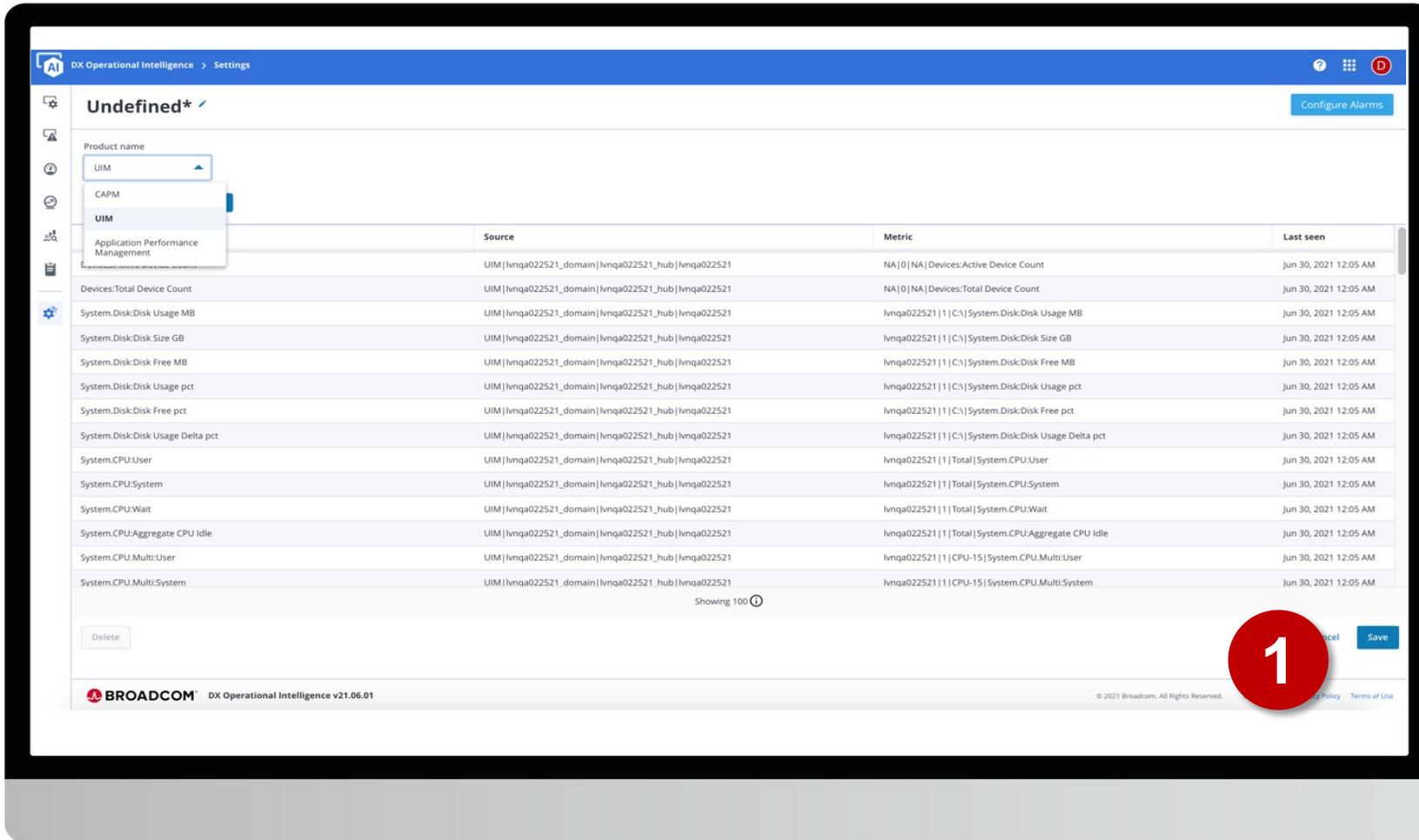
Fine Tuning Anomaly Alarms



1. To activate anomaly detection alarms, select the “Enable Detection” checkbox
2. To enable fine tuning, unselect “Use System Settings”
3. Set if detection should be below or above the dynamic threshold (or both)
4. Set the count of anomaly occurrences that raise an alarm
5. Configure the alarm message (static text and variables)
6. Select an alarm notification or create a new one with “Create New”

You can set for how many occurrences of anomalies over time/count the system should raise an alarm. This helps in further reducing the alarm noise. For example, if there are 10 instances of CPU usage spike in 15 mins then it might be a matter of concern and an alarm for it would make sense.

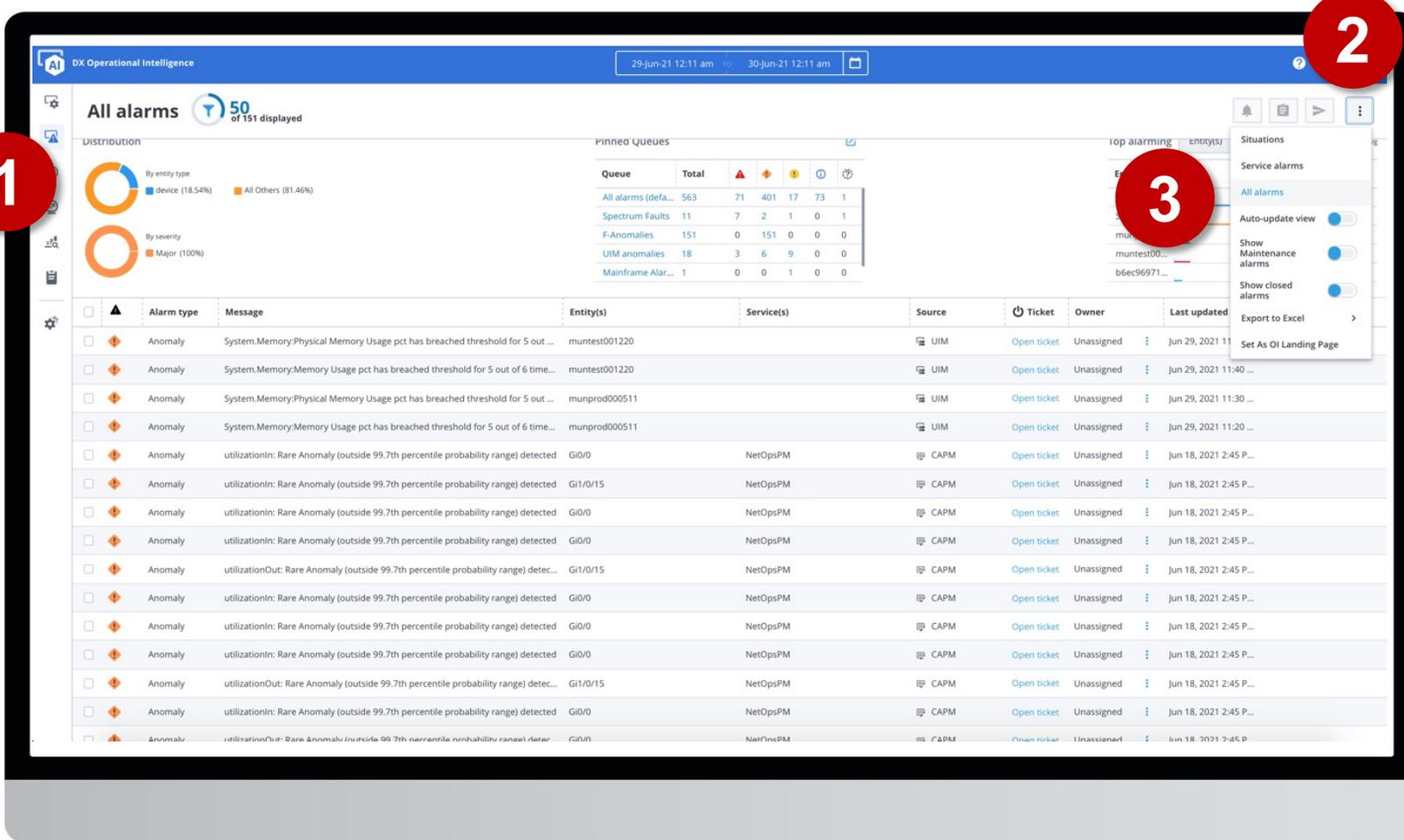
Configuring Metric Groups For Anomaly Detection #6



1. Click on the “Save” button on the metric filtering page, the Metric Monitoring Group configuration can be saved

To create the metric monitoring group, you have to first select the source product for the metrics from the drop down. This dropdown will contain all the source products for which the metrics are present in the DX Operational Intelligence repository.

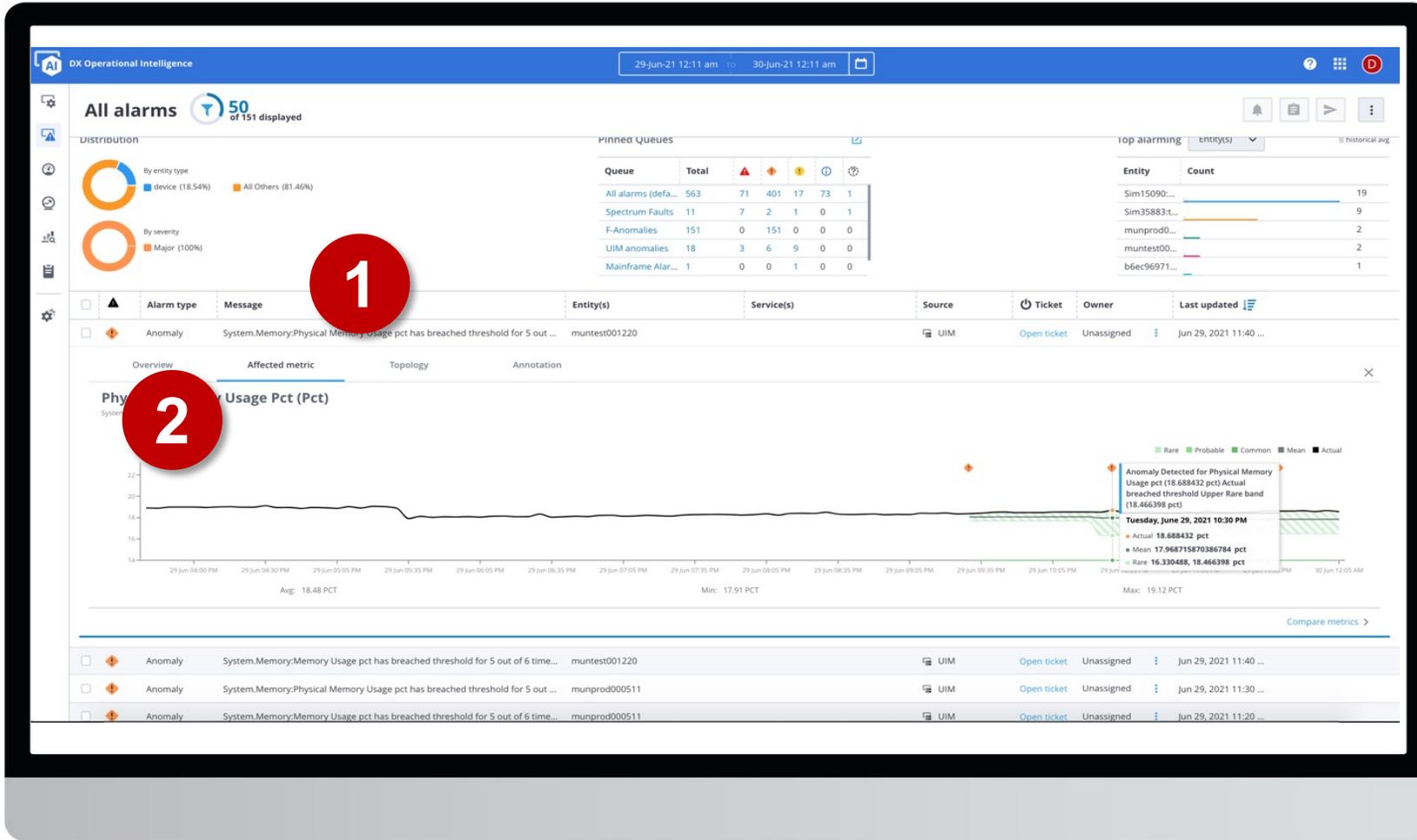
Acting On Anomaly Alarms #1



1. Click on the 2nd icon in the left navigation menu
2. Click on the three-dot menu on the top-right of the screen
3. To view the anomaly alarms, select the "All Alarms" from the menu

Once the alarms get generated, you can view and act on the alarms using Alarm Analytics in DX Operational Intelligence. Filter the alarms by selecting the "Alarm Type" as "Anomaly", to view all the Anomaly alarms in the list of alarms.

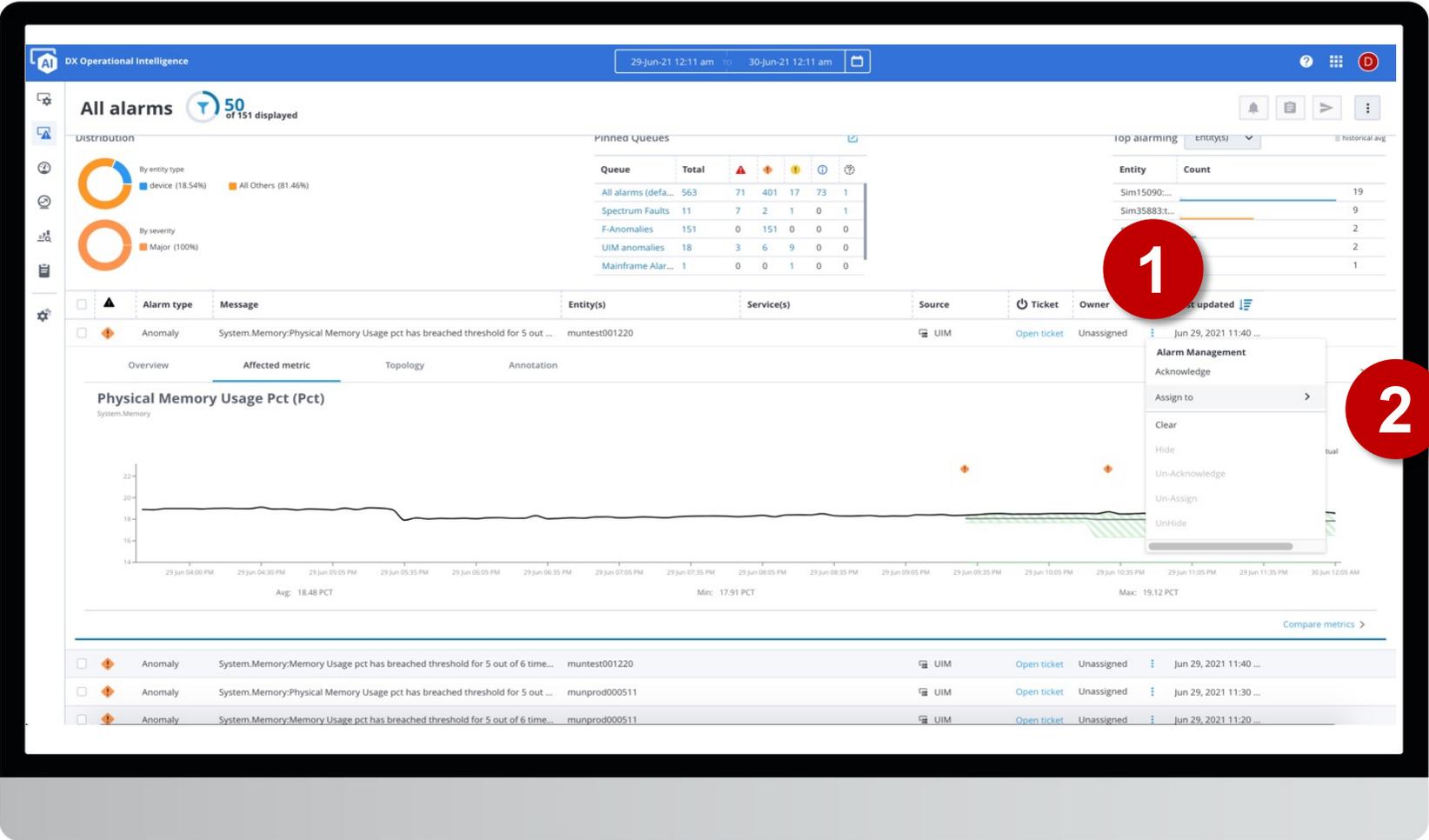
Acting On Anomaly Alarms #2



1. Click on an alarm in the list to display the expanded view
2. Select which information to display in one of the available tabs

The configured alarm message is displayed in the Message column of the table and the entity for which the anomaly has been detected for the given metric is visible in the Entity(s) column.

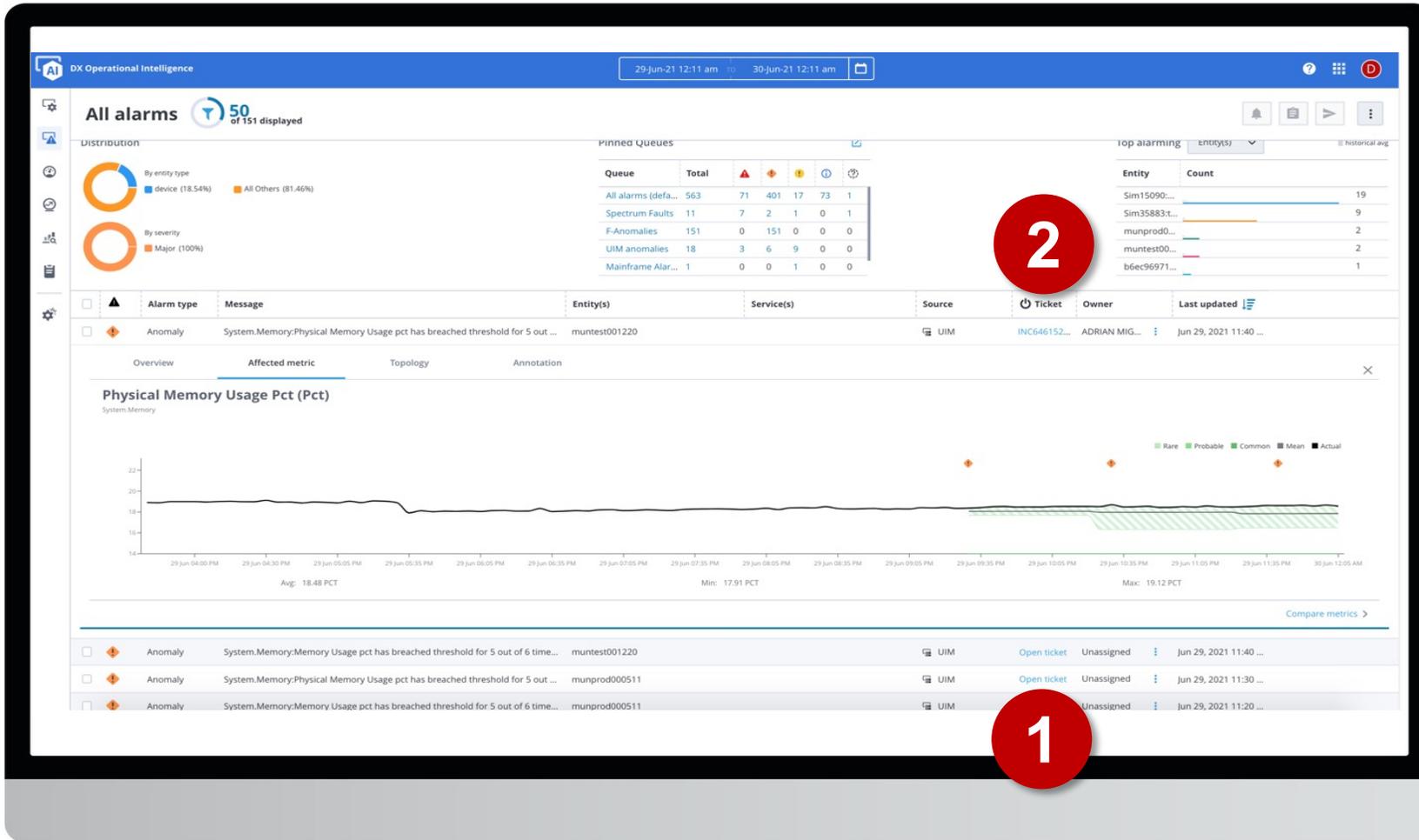
Acting On Anomaly Alarms #3



1. Click the three-dot menu next to "Unassigned" in the "Owner" column in the alarms table.
2. Select "Assign to" in the menu to make a team member owner of the alarm

Assigning an alarm to in team member make the name of the person to appear in the "Owner" column.

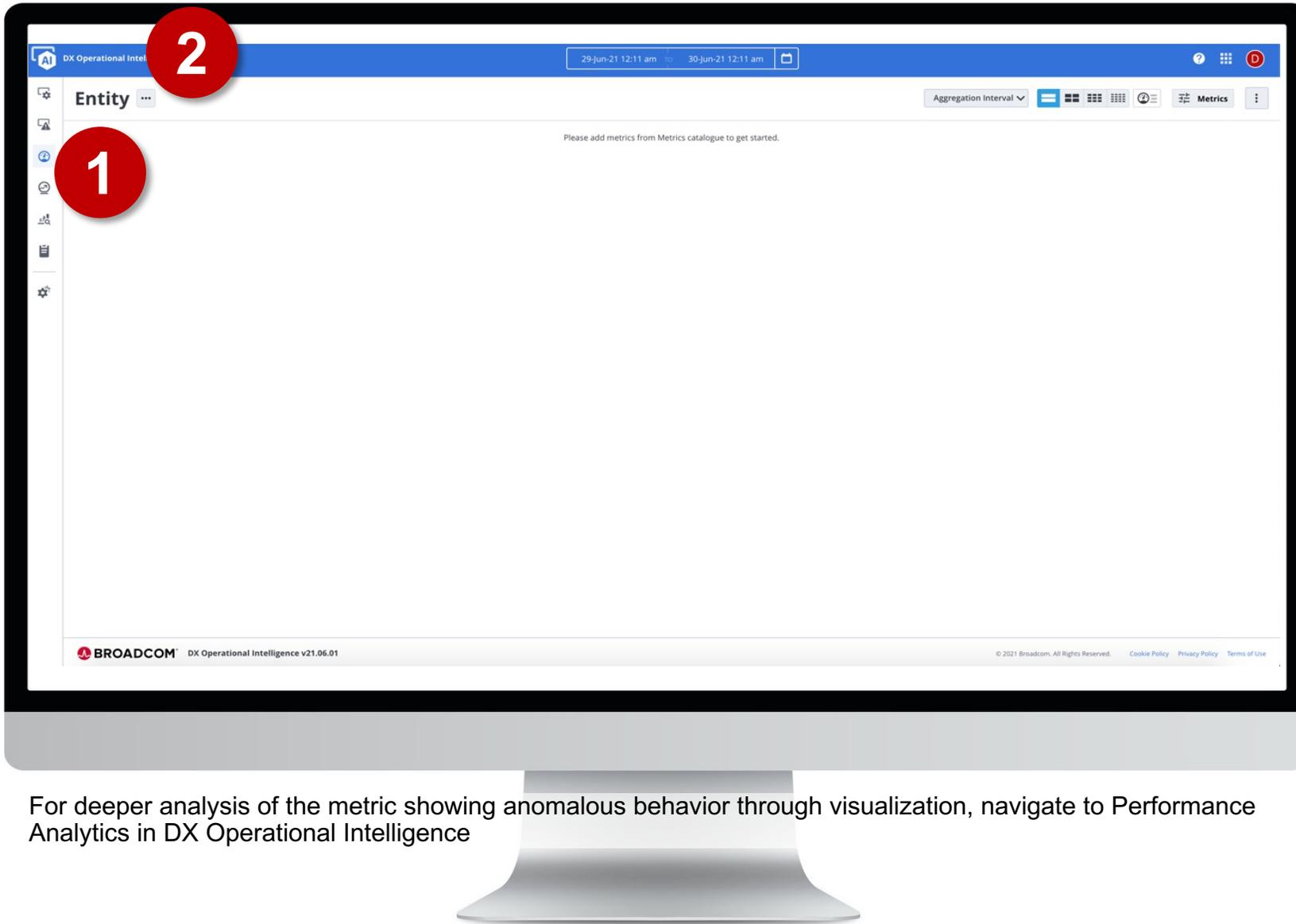
Acting On Anomaly Alarms #4



1. Create a new ticket by clicking the "Open Ticket" link in the selected alarm row
2. Check the ticket number or open an existing ticket by clicking on the ticket number in the "Ticket" column

Opening a new ticket directly from the alarm screen is possible if a Ticket Management system has been configured to the DX Operational Intelligence. This can be done from the settings menu by the Admin.

Visualizing Metrics Anomalies #1



1. Click on the third icon from the top in the left navigation menu
2. Click on the three-dot menu on the top of the screen, next to “Entity”

For deeper analysis of the metric showing anomalous behavior through visualization, navigate to Performance Analytics in DX Operational Intelligence

Visualizing Metrics Anomalies #2

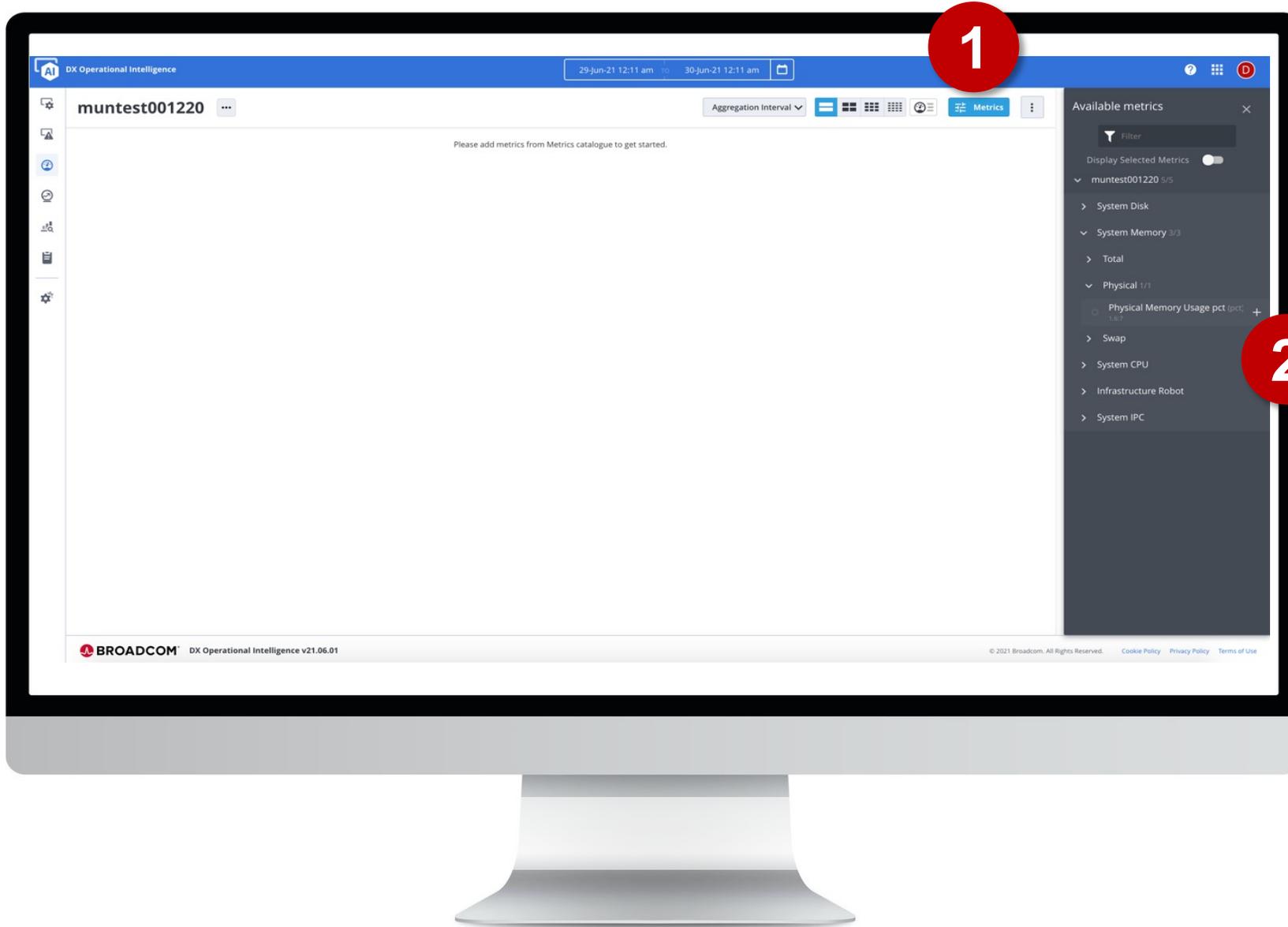
The screenshot shows a performance analytics dashboard with a table of entities. A filter is applied to the 'Entity Name' column, showing only entries containing 'muntest001220'. The table columns are State, Service, Group, Type, Identifier, and Source. The 'State' column has a dropdown menu set to 'Equals'. The 'Add' button is highlighted with a red circle labeled '2'. The selected entity is highlighted with a red circle labeled '3'. The 'Done' button is highlighted with a red circle labeled '4'. The table shows various synthetic transactions and physical devices.

State	Service	Group	Type	Identifier	Source
test7, Synthetic Transactions, Backend B...			WEBSERVICE_SERVER	Host:33cd11c56c9d	Application Performance Manageme...
Synthetic Transactions, TIXCHANGE Web...			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
Synthetic Transactions, TIXCHANGE Web...			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
/tixchange_web/shop/index.html			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
/tixchange_web/shop/newOrderForm.html			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
/tixchange_web/shop/signon.shtml			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
/tixchange_web/shop/signonForm.shtml			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
/tixchange_web/shop/viewCategory.shtml			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
/tixchange_web/shop/viewProduct.shtml			BUSINESSTRANSACTION	ServiceId:Ticketing	Application Performance Manageme...
0b0c85369669 TomcatProcess TixChange-Service			AGENT	Host:0b0c85369669	Application Performance Manageme...
10.109.34.38	VMware vCenter, Virtualization, AB-infra		vCENTER		Application Performance Manageme...
10.109.34.38			vCenter	IP:10.109.34.38	Spectrum (+1)
10.124.122.233			device	Host:10.124.122.233	CAPC
10.125.34.226			device	Host:10.125.34.226	CAPC
10.125.34.44			device	Host:10.125.34.44	CAPC
10.126.12.190			device	Host:10.126.12.190	CAPC
10.126.13.26			device	Host:10.126.13.26	CAPC
10.126.42.100			device	Host:10.126.42.100	CAPC

1. Enter a filter to select to the entity you want to display
2. Click "Add"
3. Select the filtered entity
4. Click on "Done"

The same entity name can be used to do a deeper analysis of the affected metric in Performance Analytics

Visualizing Metrics Anomalies #3



1. Click on the “Metrics” button
2. Expand the metric tree in the Available metrics slider and clicking the “+” icon for the desired metric

Visualizing Metrics Anomalies #4

1



1. Select the time range of your choice

Analyze the metric data in the selected time period and also see the anomalies detected. DX Operational Intelligence can help your operations team navigate from Anomaly to Action through a single pane of glass and helping them meet their SLAs and reduce MTTR



BROADCOM[®]

SOFTWARE