SCOM Pulse User Guide

Alert triage, object health, maintenance and dashboards for monitoring operators

Product	**SCOM Pulse**
Document version	**1.3**
Verified against the live application	**14 September 2026**
Audience	**Monitoring operators and read-only users**

Verified against a live SCOM Pulse deployment at /Pulse on a SCOM 2025 management group. Facts that could not be confirmed in that deployment are marked in the text and listed in Documentation-Verification.md.

Contents

1 About this guide **5**

1.1 Who this guide is for 5

1.2 What SCOM Pulse is, and what it is not 5

1.3 How to read a procedure 6

1.4 A note on the examples 6

2 Quick start: from sign-in to a verified action **7**

2.1 Step 1 — Open SCOM Pulse 7

2.2 Step 2 — Read the overview 8

2.3 Step 3 — Open the alert list and find the critical alert 9

2.4 Step 4 — Inspect the alert, its object and its health 9

2.5 Step 5 — Choose the appropriate action 9

2.6 Step 6 — Verify the outcome 10

3 Getting started and navigation **11**

3.1 Signing in 11

3.2 The sidebar 12

3.3 The top bar 14

3.4 Search (Ctrl + K) 14

3.5 Keyboard shortcuts 15

3.6 Service and sync status 16

4 Alert triage **18**

4.1 The alert list 18

4.2 Filtering 20

4.3 Sorting and grouping 21

4.4 Display: density, widths and columns 22

4.5 Selecting alerts 23

4.6 Rules and monitors 23

5 Investigating and acting on an alert **25**

5.1 The alert detail panel 25

5.2 Acknowledging an alert 29

5.3 Assigning an alert and recording a ticket 29

5.4 Changing resolution state and closing an alert 29

5.5 Adding a comment ... 30
5.6 Ticket and Custom Field 1–10 ... 30
5.7 Bulk actions and per-item outcomes ... 30
5.8 Reset health, diagnostics and recoveries ... 31
6 Discovered Inventory and the Health Explorer ... 33
6.1 Browsing the discovered inventory ... 33
6.2 The object page ... 34
6.3 Reading the Health Explorer ... 36
6.4 History, hosted objects, events and topology ... 37
6.5 Effective configuration ... 37
7 Performance ... 40
7.1 Choosing counters and a range ... 40
7.2 Why a chart can be empty ... 41
7.3 Pinned charts, host metrics and workload dashboards ... 41
8 Maintenance ... 42
8.1 The Maintenance page ... 42
8.2 Starting maintenance immediately ... 44
8.3 Scheduling maintenance ... 46
8.4 Extending, stopping, editing and deleting ... 48
8.5 Verifying that maintenance actually ran ... 48
8.6 Instant MM ... 49
9 Tasks ... 50
10 Rules, monitors, discoveries and overrides ... 53
10.1 Finding a workflow ... 53
10.2 Reading a workflow's properties ... 54
10.3 Overrides ... 54
10.4 Creating an override ... 55
11 Dashboards and your personal workspace ... 58
11.1 The dashboard library ... 58
11.2 Templates ... 59
11.3 Creating and editing a dashboard ... 60
11.4 Home, folders and the sidebar ... 60
11.5 Organising the sidebar ... 60

11.6 Sharing: three different things ... 60

12 Notifications ... 63

12.1 The subscription list ... 63

12.2 Creating a subscription ... 64

12.3 On-call hours live on the subscriber ... 66

12.4 Criteria Pulse will not overwrite ... 66

13 Troubleshooting and quick reference ... 67

13.1 I cannot sign in, or I am prompted for a password ... 67

13.2 I am read-only and I should not be ... 67

13.3 A number looks stale ... 69

13.4 My action failed, or only partly worked ... 69

13.5 A chart is empty ... 69

13.6 A dashboard from a management pack is missing ... 69

13.7 A resolution state I want is not offered ... 69

13.8 Something is not configurable here ... 70

13.9 End-of-shift checklist ... 70

14 Glossary ... 71

1 About this guide

SCOM Pulse is a web console for System Center Operations Manager. It gives an operator the day-to-day work — alert triage, object health, performance, maintenance windows, tasks and dashboards — in a browser, without the Operations console. This guide covers that operator's work. It does not cover installing or administering Pulse itself; that is the *SCOM Pulse Administration Guide*.

1.1 Who this guide is for

You are expected to understand basic server monitoring: what an alert is, what it means for a server to be unhealthy, and why a change window matters. You are **not** expected to have used SCOM Pulse before, and you do not need to know the Operations console.

Two kinds of reader are addressed throughout:

- **Read-only users** can see everything their permissions allow and change nothing. Every chapter's investigation sections apply to you.
- **Operators** can additionally act: acknowledge and resolve alerts, start maintenance, run tasks. Sections that require this are marked with a *Required access* box.

1.2 What SCOM Pulse is, and what it is not

SCOM Pulse reads from and writes to your existing Operations Manager management group. It is not a second monitoring system: the alerts, objects, health states, maintenance windows, rules and monitors you see are SCOM's own, and a change you make in Pulse is a change in SCOM that the Operations console will also show.

It is also not a complete replacement for the Operations console. Management pack authoring, distributed application design, complex group formulas, editing company knowledge, Run As credentials, network and UNIX/Linux discovery, connector configuration and SCOM reporting all remain console work. Where a task falls outside Pulse, this guide says so rather than leaving you looking for a button that is not there.

> **Note — How Pulse sees your data**
>
> Pulse keeps a local cache of what it has read from SCOM and refreshes it on a poll. Counts and lists are therefore accurate to the last sync, which the page tells you — for example "*Synced from SCOM with the catalog (46m ago)*". Actions you submit are queued to a background service and carried out against SCOM; they are not instant, and the interface tells you when a request has been accepted rather than pretending it has finished.

1.3 How to read a procedure

Every substantive procedure in this guide has the same shape:

Part	What it tells you
Purpose	Why you would do this, and when you would not
Required access	The SCOM profile needed — your SCOM user roles decide it, and nothing else does ("3 Getting started and navigation")
Navigation	Where the screen lives
Steps	Numbered, using the exact labels on screen
Fields	The options that matter and what they change
Expected result	What you should see, and how to confirm it independently
If it fails	The messages you are most likely to meet

Screen labels are printed **in bold** exactly as the application spells them, including its use of ⍰, ▾ and …. Paths through the interface are written **Notifications** → **Channels**. URLs keep the `/Pulse` application prefix, because that prefix is part of every link. The deployment used for this guide publishes it as `/pulse`; IIS application paths are not case-sensitive, so either spelling reaches the same page.

> **Important — Side effects are stated before the step that causes them**
>
> Where an action changes SCOM — suppressing notifications, closing an alert, overriding a workflow — the consequence is described *before* the numbered step, not after it. Read those paragraphs.

1.4 A note on the examples

The figures in this guide were captured in the dark theme from a live SCOM Pulse deployment against a SCOM 2025 management group in a lab domain, `contoso.local`, with about thirty monitored Windows and Linux computers. Host names, group names and management pack names are from that environment; yours will differ. The lab's account and host names are fictional and are shown as they appear; security identifiers have been covered with grey boxes. Nothing else in a figure has been altered: where a screen shows an empty list, a warning, or a value that looks odd, that is what the application displayed.

2 Quick start: from sign-in to a verified action

This chapter walks the whole arc of an operator's first task — open Pulse, read the overview, find the worst alert, understand what raised it, decide what to do, and verify the outcome. Each step points to the chapter that covers it properly.

2.1 Step 1 — Open SCOM Pulse

Browse to your Pulse address. In the deployment used for this guide that is `https://scom1.contoso.local/pulse`; yours is whatever your administrator published, and it may be plain `http://`.

You are not asked for a password. Pulse uses **Windows Authentication**, so your browser signs you in with the Windows account you are already logged on with. If a credential prompt does appear, see "13.1 I cannot sign in, or I am prompted for a password".

The first screen is your home dashboard. In the reviewed deployment it is a dashboard named **Operations Overview** (Figure 1), but the home dashboard is a personal setting — a colleague may land somewhere else, and so may you once you choose a different home ("11.4 Home, folders and the sidebar").

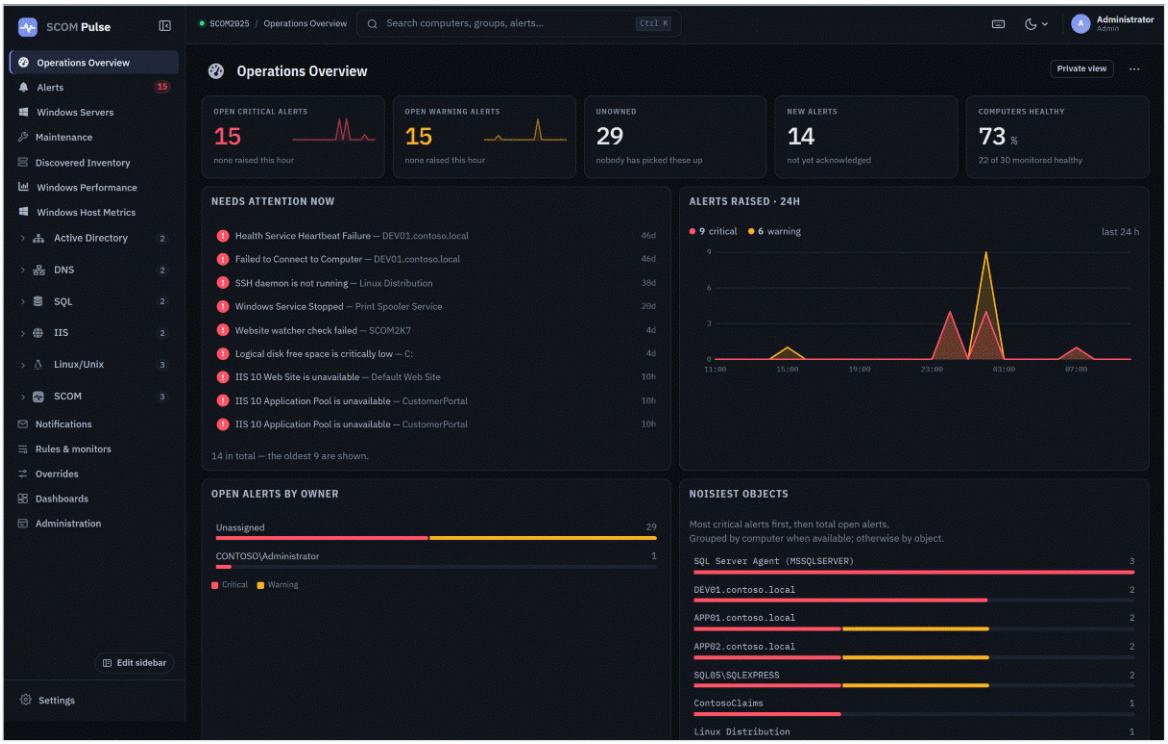


Figure 1 The home dashboard: headline numbers across the top, then the alerts most worth attention beside the 24-hour volume chart, ownership and noise below, and computer state under those.

2.2 Step 2 — Read the overview

Work down the cards. **OPEN CRITICAL ALERTS** and **OPEN WARNING ALERTS** are your queue depth. **UNOWNED** is the number nobody has taken. **NEW ALERTS** counts those not yet acknowledged. **COMPUTERS HEALTHY** is a percentage with the counts beneath it — in Figure 1, *80 %* and *24 of 30 monitored healthy*. Hover the tile for the whole picture: which computers are counted, any that nobody monitors (left out of the percentage, because a computer nobody is monitoring is not a healthy computer), and any in maintenance.

Each tile is labelled by what it counts, and every number is a link into a filtered view.

Every number is a link into a filtered view. Clicking **UNOWNED**, for example, opens the alert list already filtered to unowned alerts.

NEEDS ATTENTION NOW, directly under the headline numbers, is the fastest route into triage: it lists the alerts Pulse ranks highest, newest problem first. **ALERTS RAISED · 24H** sits beside it, with ownership, the noisiest objects and computer state below.

2.3 Step 3 — Open the alert list and find the critical alert

Click **Alerts** in the sidebar, or click a counter card. The alert list (Figure 6) opens on active alerts, grouped by severity and sorted by **Smart rank** within each group.

Set the view to what you actually want to work: click **Active**, then in the filter rail tick **Critical** under **SEVERITY**. The heading above the grid updates to tell you how many alerts match.

2.4 Step 4 — Inspect the alert, its object and its health

Click the alert row. A detail panel opens on the right (Figure 10). Read three things before you touch anything:

1. **ALERT DESCRIPTION** — what the management pack says went wrong.
2. **WHY THIS FIRED** — whether a **rule** or a **monitor** raised it, and what that means for closing it. This distinction decides your next move; see "4.6 Rules and monitors".
3. **HEALTH & TECHNICAL CONTEXT** — the state of the object right now, which is not always the state that raised the alert.

2.5 Step 5 — Choose the appropriate action

- If a **monitor** raised it, the alert closes itself when the monitor goes healthy. Fix the cause. Closing the alert by hand does not fix the state, and SCOM 2019 and later refuse the close while the monitor is still warning or critical.
- If a **rule** raised it, nothing will ever close it automatically. Deal with the underlying event, then close the alert.
- If you are starting work and want to stop the noise while you do, **acknowledge** it and assign it to yourself so the rest of the team can see it is taken.
- If the server is about to be worked on deliberately, put it in **maintenance** instead of closing alerts ("8 Maintenance").

> **Caution — Do not reset health to make an alert go away**
>
> **Reset health** tells SCOM to recalculate a monitor's state. It is a legitimate step after you have fixed the cause and the monitor has not noticed yet. It is not a way to clear your queue: if the underlying problem is still there, the monitor will go critical again, and in the meantime you have thrown away the evidence of when the state actually changed.

2.6 Step 6 — Verify the outcome

Pulse queues your action and reports what SCOM said about it. Verify rather than assume:

1. Watch for the confirmation. A bulk action reports **per-target outcomes**, not one overall verdict — three of five targets can succeed.
2. Re-open the alert. The **RESOLUTION STATE** and the **EVENT TIMELINE** should both show your change, attributed to you.
3. For maintenance, confirm the window is actually running on the **Maintenance** page and on the object's **Maintenance** tab — a scheduled occurrence is a projection, not proof it ran ("8.5 Verifying that maintenance actually ran").

> **Note — Your name, SCOM's name**
>
> Every write reaches SCOM as the Pulse **service account**, while Pulse separately records who asked. So an alert you acknowledge shows the service account as the modifying user in SCOM, and your account in the Pulse timeline and audit trail. That is expected, not a fault.

3 Getting started and navigation

3.1 Signing in

Pulse authenticates with Windows Authentication and never asks for a password of its own. What you can see and do once signed in comes from your **SCOM user roles** and nothing else. There is no separate list of Pulse users and nothing for anyone to grant you in Pulse itself: you see what your SCOM user roles cover and may do what their profiles allow — the same answer the Operations console gives.

Your SCOM profile	In SCOM Pulse
Read-Only Operator	You see everything in the role's scope, including an alert's history and knowledge and an object's monitors, events and performance. You cannot act
Operator	Alerts — acknowledge, resolve, set any resolution state, comment, owner, ticket; maintenance mode and maintenance schedules; tasks in the role's task scope; diagnostics and recoveries; the notification subscriptions that notify only you
Advanced Operator	Everything an Operator can do, plus overrides on objects and groups in the role's scope
Author	Everything an Advanced Operator can do, plus class-wide overrides and group authoring
Read-Only Administrator (SCOM 2022 and later)	You monitor like a Read-Only Operator, and you can read the whole **Administration** page, the **Management servers** page and every notification subscription. You change nothing, and **Settings** does not open
A role made from **Delegated Administrator** (SCOM 2022 and later)	You can read the **Administration** page, and change exactly what your SCOM administrator ticked for the role in the console — repairing agents, say, and nothing else
Administrator	Everything, including **Administration**, **Settings**, the audit trail and the licence key. A SCOM Administrator is the only kind of SCOM Pulse administrator
No SCOM user role, or only a report or Application Monitoring role	You can sign in, and you see nothing

Four things follow from that:

- **Several roles add up for seeing, not for acting.** If you are in several SCOM user roles you see the union of what they cover, but you may act only where a role that grants the action reaches: what one

role grants is never added to what another covers. A Read-Only Operator role over everything plus an Operator role over the SQL group lets you see everything and act on SQL only.

- **Viewer, Operator and Admin are a summary, not a grant.** Those words appear in the account chip at the top right and on the **Your access** page. They summarise your SCOM profile — Administrator reads as **Admin**; Operator, Advanced Operator and Author read as **Operator**; Read-Only Operator reads as **Viewer** — and nobody assigns them separately.
- Group membership comes from the **logon token Windows built when you signed in to Windows**. If an administrator adds you to a group that a SCOM user role names, closing and re-opening the browser is not enough — you must sign out of Windows and back in. A change to the SCOM user role itself reaches Pulse within about a minute.
- **Being able to sign in is not by itself permission to see monitoring data.** Someone who holds no SCOM user role sees nothing and is told so: they land on an **Access status** page, which says whether Pulse is still waiting to read the SCOM user roles or the account holds none, and whom to ask. If that is you, see "13.2 I am read-only and I should not be".

You can always see the decision Pulse made about you, and every test behind it, at **/Pulse/Access** — see "13.2 I am read-only and I should not be".

3.2 The sidebar

The sidebar (Figure 2) is your navigation. In the reviewed deployment it held, in order: **Operations Overview**, **Alerts**, **Windows Servers**, **Maintenance**, **Discovered Inventory**, **Windows Performance**, **Windows Host Metrics**, folders for **Active Directory**, **DNS**, **SQL**, **IIS**, **Linux/Unix** and **SCOM**, then **Notifications**, **Rules & monitors**, **Overrides**, **Dashboards**, **Administration** and **Settings**.

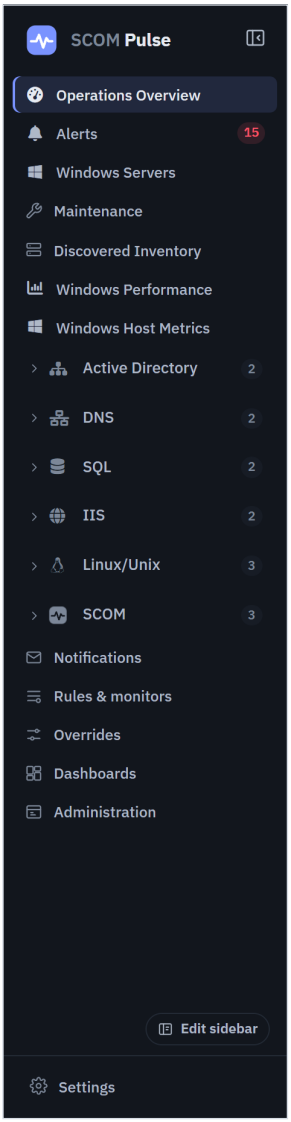


Figure 2 The sidebar, with workload folders expanded and the alert count badge beside **Alerts**.

Three things about that list matter:

- **It is personal.** Most sidebar entries are dashboards you or an administrator put there. Yours will differ, and the entries are organised on the **Dashboards** → **Sidebar** tab ("11.5 Organising the sidebar").
- **Workload folders depend on management packs.** The **SQL** or **IIS** folders are useful only where those management packs are installed and collecting.
- **Some entries are hidden by permission. Administration** and **Settings** appear only for accounts allowed to reach them. Not seeing them is a permissions answer, not a fault.

Collapse and expand the sidebar with the menu button at its top. Folders expand and collapse individually.

3.3 The top bar



Figure 3 The top bar: management group and page breadcrumb on the left; search, keyboard shortcuts and the theme button on the right. **My actions** is hidden here because nothing was in flight.

- The **breadcrumb** names the management group and the page you are on.
- **Search** (**Ctrl + K**) is described below.
- **My actions** shows the actions you have queued recently and how they ended — the quickest way to confirm that something you submitted actually landed. It appears only when there is something to show; on a quiet system it is hidden, and its tooltip reads "*0 in flight, 0 failed in the last hour*". If you cannot find it, nothing of yours is outstanding.
- **Keyboard shortcuts** opens the shortcut list (Figure 5).
- **Theme** is the sun/moon button in the top bar. Open it to choose Light, Dark, or Use system setting. Use system setting follows your computer or browser appearance and responds when it changes. A checkmark shows your choice. Your choice is remembered in this browser; until you choose, the site default applies. Administrators set that default under **Settings** → **Site & display**.

At the bottom of the window a status bar reports the counts on the current page, how many rows you have selected, and the health of the Pulse service and its sync. If that service indicator is not healthy, what you are looking at may be stale; see "13.3 A number looks stale".

3.4 Search (Ctrl + K)

Press **Ctrl + K** anywhere, or click the search box. Type part of a computer, group or alert name and Pulse offers matches across objects and alerts as you type (Figure 4). Press **Enter** on a result to open it.

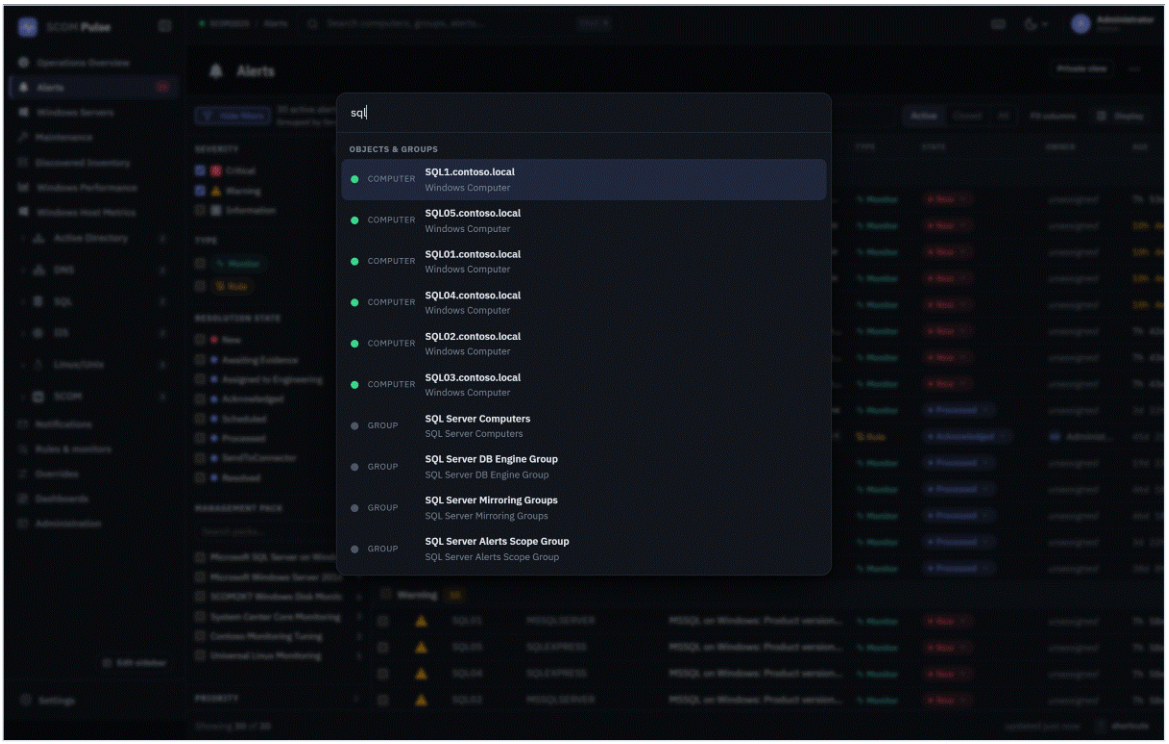


Figure 4 The command palette, opened with **Ctrl + K** and filtered by typing part of a computer name.

This is the fastest way to get to a specific server. It is not a substitute for the filters on the alert list, which is where you work a queue rather than find one thing.

3.5 Keyboard shortcuts

Click the keyboard shortcuts button in the top bar for the list the application actually offers (Figure 5). Use that panel rather than a printed list: it is generated from what this build supports.

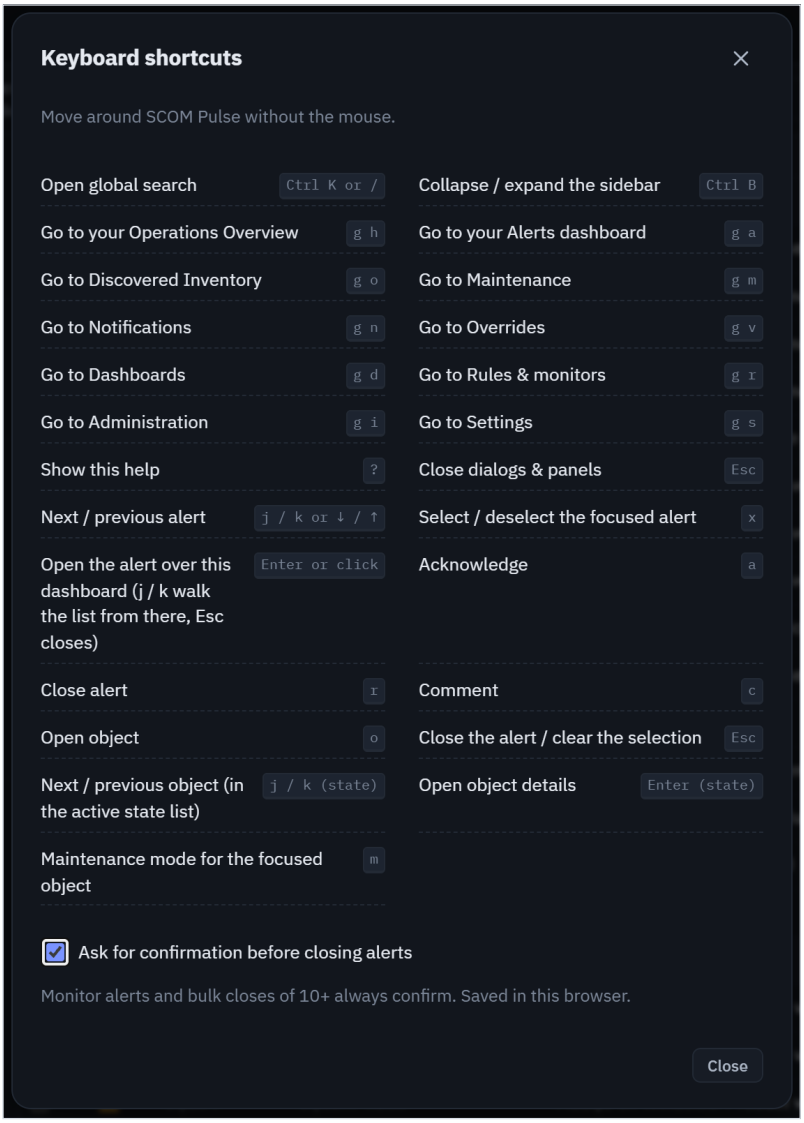


Figure 5 The keyboard shortcuts panel, opened from the top bar.

3.6 Service and sync status

Pages that read cached data say when they last read it — "*Synced from SCOM with the catalog (46m ago)*" on **Notifications**, "*read from the cache (synced 46m ago)*" on **Administration**, "*Synced with the catalog 46m ago*" on **Rules & monitors**. Not everything on a page was read at the same moment: on the **Watchers** tab, for example, a line under the list says when the watcher objects were last read from SCOM,

and that the time under the page title is when the Administration inventory was last read, so the two can differ. When a number looks wrong, check when it was read before you chase the data.

4 Alert triage

The **Alerts** page — the Alert Center — is where an operator spends most of a shift. This chapter covers finding the right alerts; the next covers acting on them.

4.1 The alert list

Open **Alerts** in the sidebar, or `/Pulse/Alerts`.

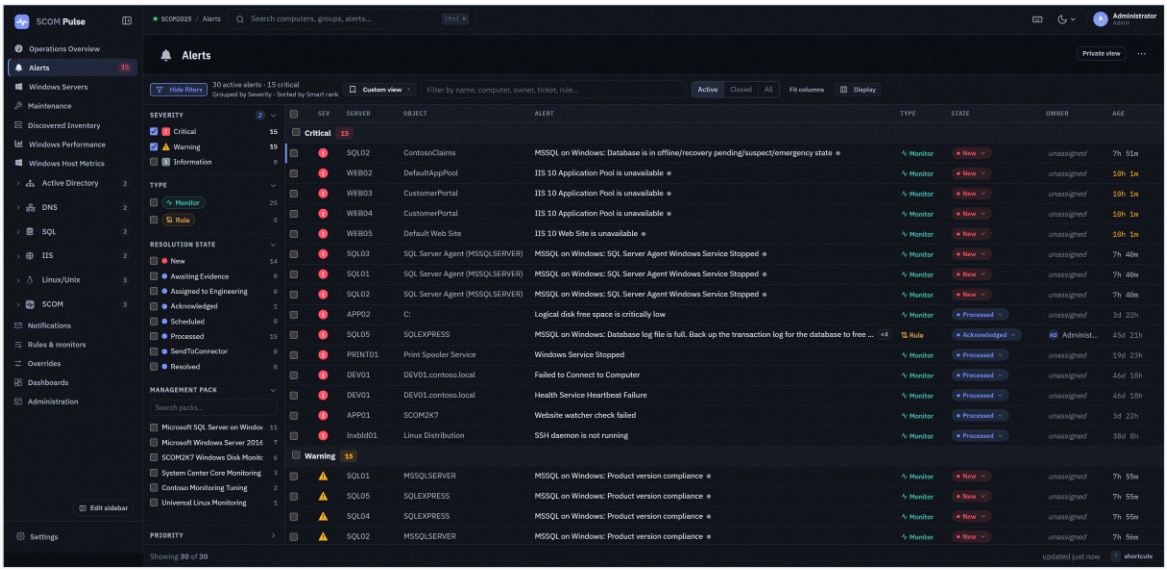


Figure 6 The Alert Center, grouped by severity. The filter rail is on the left, the match count, grouping and sort above the grid, and **Fit columns** and **Display** on the right.

Above the grid:

- **Active**, **Closed**, **All** choose which alerts are in scope at all. **Active** is the working queue.
- The heading counts what matched — "*18 active alerts · 6 critical*".
- **Grouped by Severity · Sorted by Smart rank** says how the rows are arranged; click it for the grouping and sort controls ("4.3 Sorting and grouping").
- **Custom view** / **Private view** indicates that the current combination of filters is a saved personal view, not the shipped default.
- **Hide filters** collapses the filter rail.
- **Fit columns** sizes the visible columns to the grid in one pass ("4.4 Display: density, widths and columns").
- **Display** opens density, width and column options.

Each row shows:

- **SEV** — the severity icon.
- **SERVER** — the computer the alert is on, by its short name. When SCOM names no computer for the alert (a SQL database, a web site, a Linux heartbeat watcher), Pulse works it out from SCOM's own relationships: the object's hosting chain, or the single computer that contains it. **Unknown** means no such computer could be found; **Not applicable** is shown for groups, distributed applications and the management group, which have no single server. On a newly upgraded installation servers fill in over the first few alert syncs.
- **OBJECT** — the object that raised the alert, by its own name: the database or instance, the web site, or the computer's full name for an alert on the computer itself.
- **ALERT** — the alert name. A ×2 beside it is its **repeat count** — one alert that has fired twice, not two alerts.
- **TYPE** — whether a **Rule** or a **Monitor** raised it.
- **STATE**, **OWNER** and **AGE**. The Age colour says how long the alert has been open: dark under an hour, grey from 1 to 8 hours, amber from 8 hours to 3 days — still open after a shift — and light grey beyond 3 days. It is not an SLA or overdue marker; hover the Age header or cell for the key.

The older stacked **Source / Path** column is still available under **Display**.

4.2 Filtering

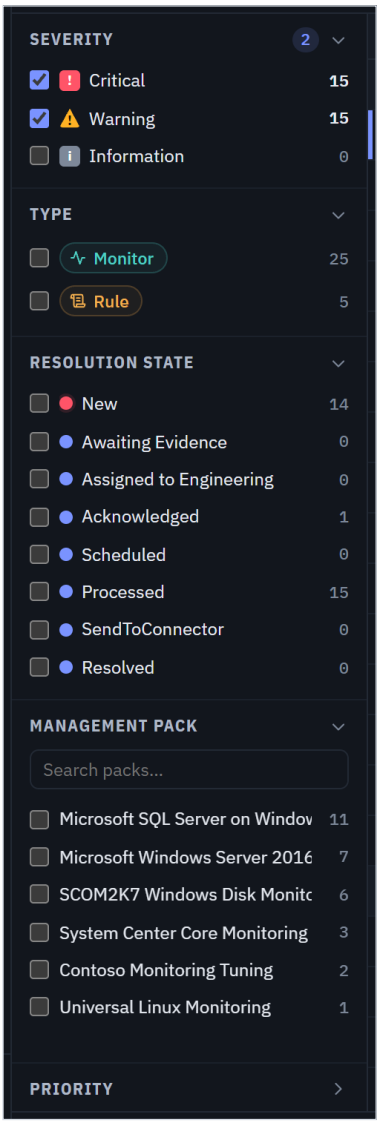


Figure 7 The filter rail. Each facet shows how many alerts carry that value in the current scope.

The rail offers, in order:

Facet	Values seen in the reviewed deployment
SEVERITY	**Critical**, **Warning**, **Information**

Facet	Values seen in the reviewed deployment
TYPE	**Monitor**, **Rule**
RESOLUTION STATE	**New**, **Acknowledged**, **Scheduled**, **Resolved**, plus the states your management group defines — in the reviewed deployment also **Awaiting Evidence** and **Assigned to Engineering**
MANAGEMENT PACK	Every pack that raised a matching alert, with counts
PRIORITY	High, Medium, Low
AGE	Age bands
QUICK FILTERS	Shortcuts such as unowned alerts

Resolution states are a management group setting, not a Pulse list: yours will be different, and an administrator can shorten the list the **Set state** menu offers ("13.7 A resolution state I want is not offered").

Search, above the rail, matches alert text. Owner, group and class filters are reached from the same rail and from the links on the overview cards.

> **Important — The count in the heading is not the number of rows on screen**
>
> The heading counts everything that matches your filters. The grid renders a page of that set and loads more as you scroll. Selection follows the grid, not the filter — see "4.5 Selecting alerts".

4.3 Sorting and grouping

Click **Grouped by Severity · Sorted by Smart rank** above the grid, and the **DISPLAY** section of the filter rail opens with both controls.

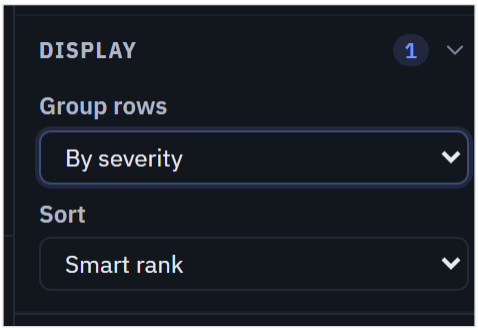


Figure 8 The **DISPLAY** section of the filter rail: how rows are grouped, and how they are sorted within each group.

Group rows offers **No grouping**, **By object**, **By computer**, **By rule / monitor** and **By severity**. Grouped by severity, the rows fall under **Critical**, **Warning** and **Information** headings, each with a count badge in its severity colour, and the sort applies within each group. A new **Alerts** dashboard is grouped by severity; an existing dashboard or saved view keeps the grouping it stored. Grouping is presentation, not a filter: it does not count as an active filter, and **Clear all filters** leaves it alone. Choose **No grouping** for a single list.

Sort offers **Smart rank**, **Newest**, **Oldest**, **Severity**, **Most repeated**, **Recently modified** and **Object**.

Smart rank is the default. Smart rank orders by how much an alert is likely to matter — severity, age, repeat count, whether the object belongs to a group pinned on the Overview — rather than by time alone. It is the right default for a queue you have not seen before.

Switch to a time sort when you need chronology: a newest-first sort answers "what just broke", which Smart rank deliberately does not.

Column choices live under **Display**.

4.4 Display: density, widths and columns

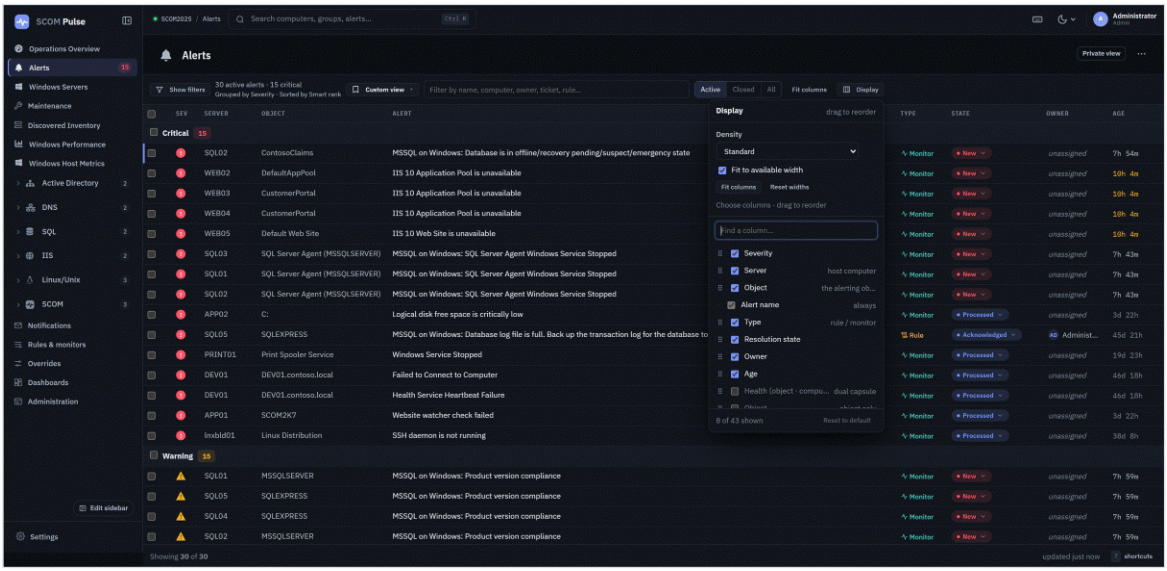


Figure 9 The **Display** menu over the alert list: density, the width controls, and the column chooser.

Display controls how much fits on screen:

- **Density** — **Compact**, **Standard** or **Comfortable** rows.
- **Fit to available width** — on unless you turn it off. Width that would otherwise sit empty goes to **Object**, as much as its names need up to half, and the rest to **Alert**. Widths you dragged stay as minimums.
- **Fit columns** — also beside **Display** on the toolbar. It sizes every visible column to the grid in one pass: compact columns get what their header and values need, and **Object** and **Alert** share the rest. The confirmation, "*Columns fitted*", offers **Undo**.
- **Reset widths** — returns every column to its default width.
- **Choose columns** — tick columns to show them and drag to reorder; **Find a column** searches the list. The grid ships with 8 of 43 columns shown, and **Reset to default** returns to them. The rest include **Source / Path**, **Computer**, **Class**, **Priority**, **Repeat count**, **Created**, **Ticket**, **Maintenance mode**, **Latency**, **Last modified by**, **Connector**, **Forwarding status** and the ten custom fields.

Columns can also be resized by dragging the edge of a column header. These are personal preferences and are remembered for you; they change nothing in SCOM and nothing for anyone else.

4.5 Selecting alerts

Tick the checkbox on a row to select it. Use the header checkbox to select the rows currently loaded.

> **Caution — "Select all" means the rows that are loaded**
>
> Selecting from the header selects the alerts the grid has loaded, which is not necessarily every alert that matches your filter. Before a bulk action, check the selection count in the status bar against the number you intend to change. If they differ, narrow the filter until the whole matching set is loaded, or work in batches.

4.6 Rules and monitors

Every alert is raised either by a **rule** or by a **monitor**, and the difference decides how it ends.

	Rule alert	Monitor alert
What raised it	An event or performance rule matched	A monitor changed health state
Health state behind it	None	Yes — the monitor's state
Closes automatically	Never	Yes, when the monitor returns to healthy
Right way to end it	Deal with the cause, then close the alert	Fix the cause; the alert closes itself

	Rule alert	Monitor alert
Closing it by hand	Appropriate once handled	Does not fix the state; SCOM 2019 and later refuse the close while the monitor is still warning or critical

Pulse states this on the alert itself, in **WHY THIS FIRED**, using the words above. When you are unsure, read that box.

5 Investigating and acting on an alert

5.1 The alert detail panel

Click any row to open the detail panel.

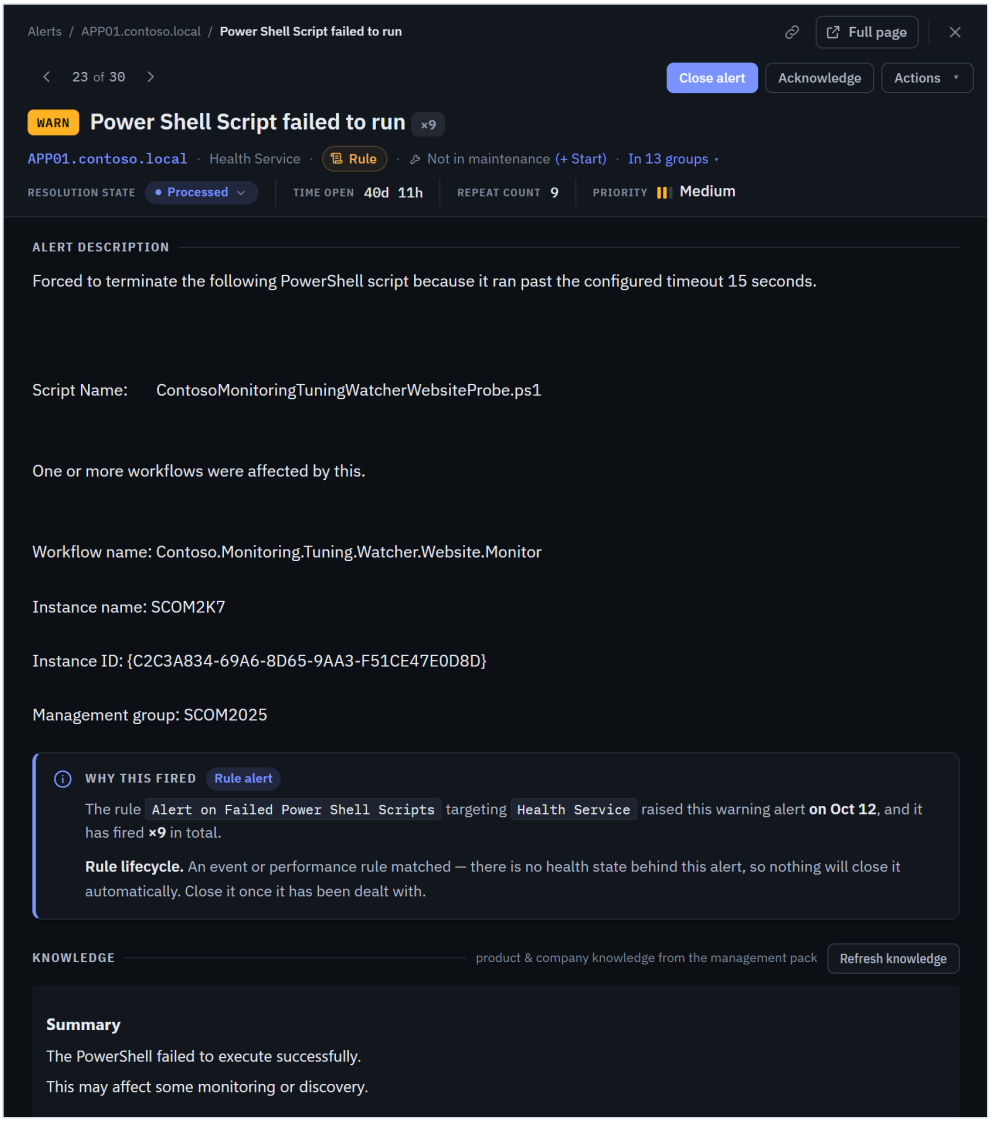


Figure 10 A **rule** alert's detail panel: identity and state at the top, then the description, why it fired, knowledge, and the health and technical context. A rule alert offers **Close alert**; a monitor alert offers **Reset health** instead (Figure 11).

Across the top: a breadcrumb, **Full page** to open the alert on its own page, a position indicator (**1 of 28**) with arrows to walk the filtered set without going back to the grid, and the action buttons — **Close alert** on rule alerts, **Reset health** on monitor alerts, **Acknowledge**, and **Actions** .

Below that, the alert's identity: severity badge, name, source object, the object's class, a **Monitor** or **Rule** chip, its maintenance state with a **(+ Start)** shortcut, and the groups the object belongs to. Then **RESOLUTION STATE**, **TIME OPEN**, **REPEAT COUNT** and **PRIORITY**.

The body holds, in order:

- **ALERT DESCRIPTION** — the management pack's own text.
- **WHY THIS FIRED** — rule or monitor, what raised it, when, how often, and the lifecycle consequence (Figure 11).
- **KNOWLEDGE** — product and company knowledge from the management pack where it exists. Where it does not, the panel says "*No runbook knowledge attached*". Pulse displays knowledge; editing company knowledge remains Operations console work.
- **HEALTH & TECHNICAL CONTEXT** — the **Health Explorer itself**, mounted in the panel. Since 1.2.8 this is the real monitor hierarchy, not a summary: the same tree, the same counts ("*6 monitors (1 unit, 5 rollup) · no unhealthy monitors reported on this object*"), the same **Refresh**, and the same per-monitor actions you get on the object page. The host name is a link to the object's own page where the object is known. Triage is exactly when you want the monitor tree and exactly when you least want to lose your place, so it comes to you.
- **ALERT CONTEXT** — the raw property bag from the event that raised it.
- **EVENT TIMELINE** — every state change with who made it (Figure 12).
- **ASSIGNMENT** — owner and ticket.
- **NEXT STEPS** — **Put in maintenance mode**, **Run agent task**, **Create override**.
- **COMMENTS** — team notes on this alert.
- **OTHER OPEN ALERTS ON** *(the object)* — the neighbouring noise, with a link to all of it.
- **Custom fields** and the **MANAGEMENT PACK** properties of the rule or monitor, with **All alerts from this rule** →.

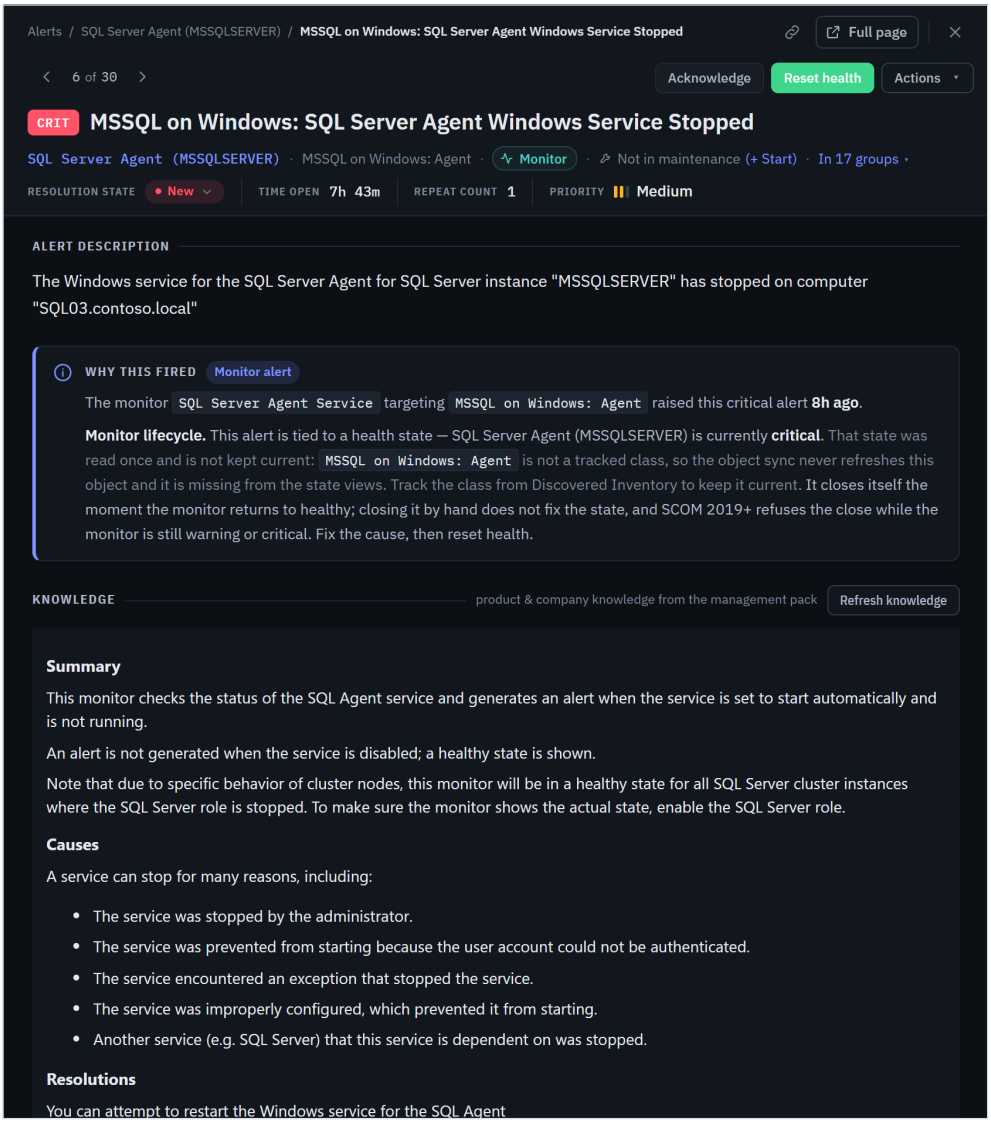


Figure 11 WHY THIS FIRED for a **monitor** alert, stating the lifecycle consequence directly — and note **Reset health** in place of the rule alert's **Close alert**.

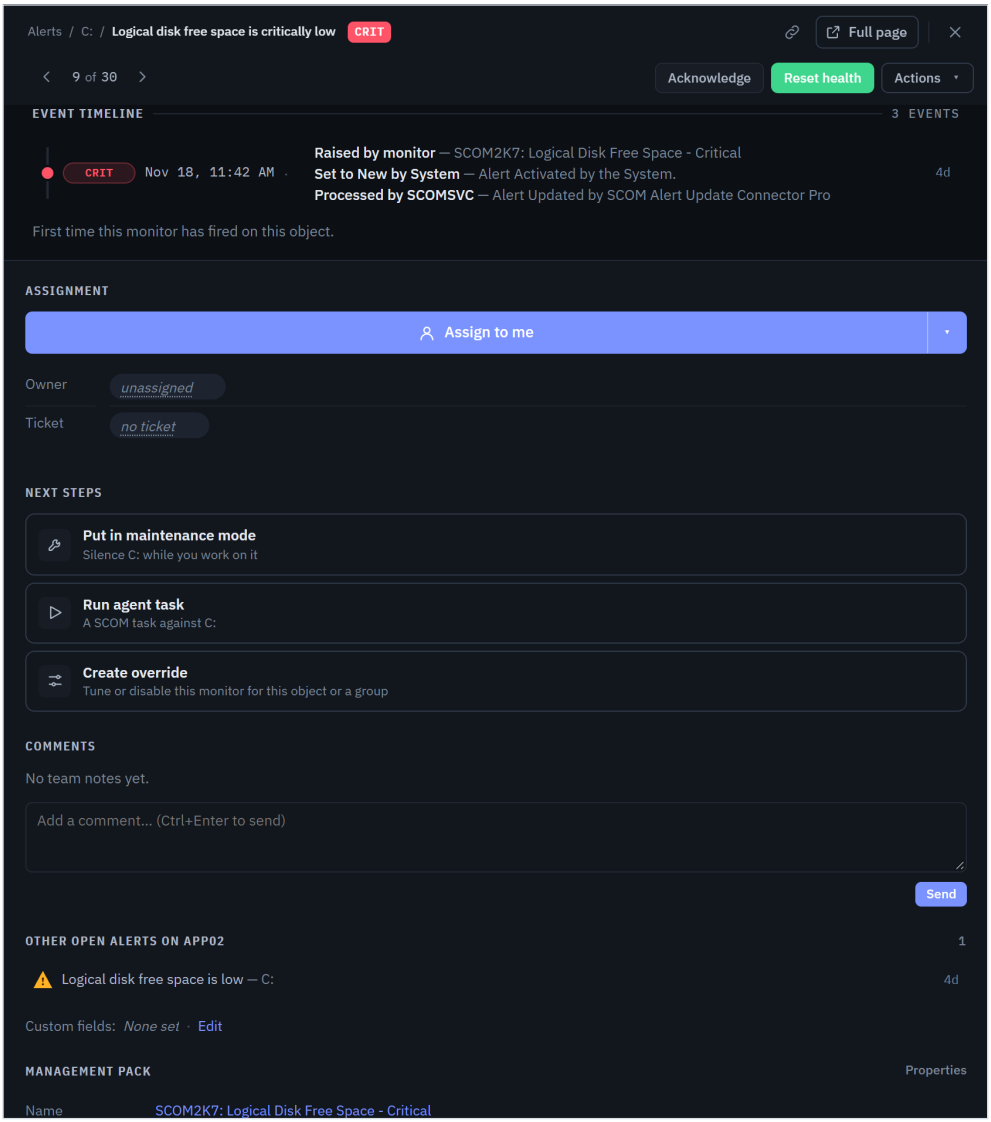


Figure 12 The event timeline and assignment area: each event, what caused it and when, then the owner and ticket.

5.2 Acknowledging an alert

> **Required access — Operator profile or better, on objects your role covers**
>
> Acknowledging writes to SCOM. A Read-Only Operator cannot do it, and the role that gives you the Operator profile must cover the object the alert is on: seeing an alert through a read-only role does not let an Operator role elsewhere act on it.

Purpose — tell the rest of the team that this alert is being looked at.

Navigation — **Alerts** → select the alert.

1. Open the alert, or tick its checkbox in the grid.
2. Click **Acknowledge**.
3. Watch for the confirmation.

What it changes — the alert's **RESOLUTION STATE** moves to the state your administrator has mapped to Acknowledge. That mapping is configurable: in the reviewed deployment **Acknowledge** sets **Acknowledged (249)**, but it may be a different state in yours.

How to verify — re-open the alert. The new state shows at the top and a new entry appears in the **EVENT TIMELINE** attributed to you.

5.3 Assigning an alert and recording a ticket

In the **ASSIGNMENT** section, use the owner control to take the alert (**Assigned to you**) or hand it to someone else, and the **Ticket** field to record your ticket reference. Owner is one of the alert list's columns, so an assigned alert stops showing as unowned on the overview.

5.4 Changing resolution state and closing an alert

> **Required access — Operator profile or better, on objects your role covers**

1. Open the alert.
2. Open the **RESOLUTION STATE** control, or use **Actions** .
3. Choose the state.

The list you are offered may be a shortlist: an administrator can pick which resolution states the menu offers, for everyone. That shortens the menu and is not a permission — if your role may update the alert, you may set any state the management group has. **Closed** is always offered, because it is the Close action.

Caution — Closing a monitor alert is not fixing the monitor

Closing a monitor alert does not change the monitor's health state. The monitor is still warning or critical, it will raise again, and SCOM 2019 and later will refuse the close outright while the state persists. Fix the cause. If the cause is genuinely gone and the monitor has not noticed, use **Reset health** ("5.8 Reset health, diagnostics and recoveries") — knowing that it discards the state-change evidence.

5.5 Adding a comment

Use **COMMENTS** to leave a note on the alert for whoever picks it up next. Comments are visible to everyone who can see the alert. Your account is recorded automatically, and in this deployment Pulse appends a configurable suffix — "*via SCOM Pulse*" — to the comments it writes into SCOM.

5.6 Ticket and Custom Field 1–10

SCOM gives every alert a ticket ID and ten custom fields; management packs and connectors use them, and so do most ticketing integrations. Edit them from **Custom fields: … · Edit** at the foot of the detail panel.

Important — Custom fields may be a connector's working storage

If a connector integrates SCOM with a ticketing system, a custom field may be the field that connector reads or writes. Ask before you repurpose one.

5.7 Bulk actions and per-item outcomes

Required access — Operator profile or better, on objects your role covers

1. Tick the alerts you want in the grid. The status bar shows the running count.
2. Re-read "4.5 Selecting alerts" and confirm that count is what you intend.
3. Use the action bar that appears for the selection: **Acknowledge**, **Close**, **Reset health…**, **Set owner…** and **Maintenance mode…**, with **Set state…**, **Comment…**, **Ticket…** and **Custom fields…** under **More** . **Reset health…** is available only when every selected alert is an open monitor alert, up to 10 at a time; hover it to see why it is unavailable.
4. Review the confirmation before submitting.

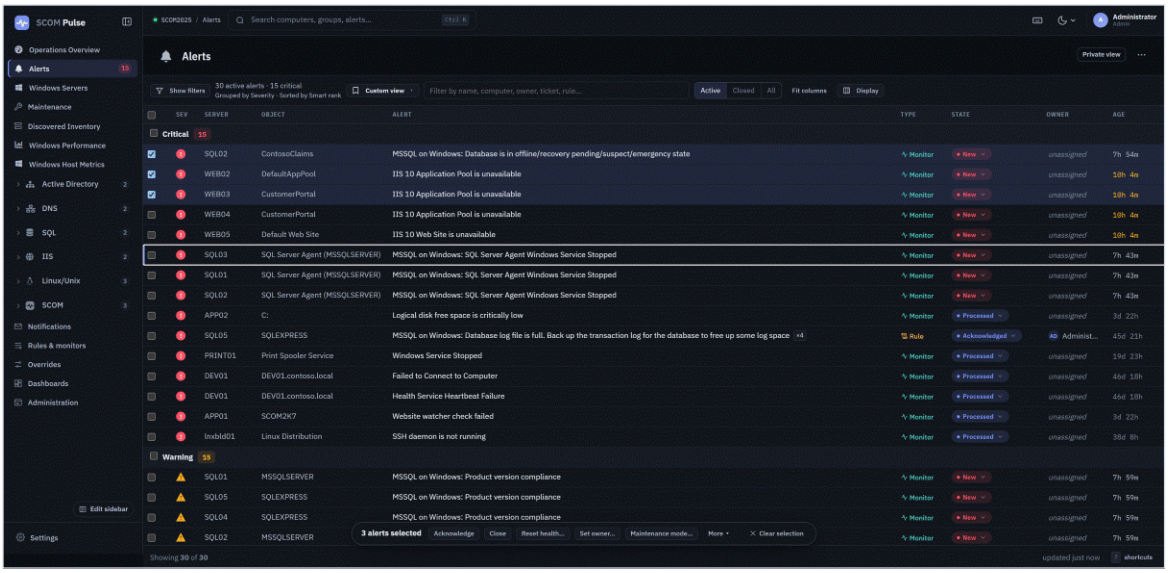


Figure 13 Three monitor alerts selected, with the bulk action bar at the foot of the grid. Nothing has been submitted.

Expected result — the request is queued, and Pulse reports the outcome **per target**. A bulk action is not atomic: some alerts can succeed while others fail, typically because an object is out of your SCOM scope or because SCOM refused a close on a still-unhealthy monitor. Read the per-item results rather than the overall banner, and check **My actions** in the top bar afterwards.

5.8 Reset health, diagnostics and recoveries

> **Required access — Operator profile or better, on objects your role covers**
>
> Resetting health and running diagnostics or recoveries are stronger than acknowledging an alert — they change a monitor's state or the monitored system itself — but they need the same profile: a SCOM user role with the Operator profile or better that covers the object. A Read-Only Operator can read the monitor tree and cannot run any of them.

Reset health asks SCOM to reset a monitor to healthy. Use it after you have fixed the cause and the monitor has not re-evaluated yet. It is available on a monitor alert's detail panel, from the Health Explorer, and on the alert grid's action bar for up to 10 open monitor alerts at once.

Before anything is reset, Pulse shows a preview of exactly which monitors it will reset. A rollup monitor is never reset directly: Pulse walks down the selected branch, follows dependency monitors onto the objects they depend on, and lists the unhealthy **unit** monitors underneath, each once. Confirm that list and only that list is reset, once, through the audited action queue; a preview left open for more than two minutes

has to be made again. Pulse resets nothing if the selection includes a rule alert, reaches more than 10 unit monitors, touches an object outside your scope, or meets a dependency list SCOM could not read completely or that loops back on itself.

A reset is a real health change: if the fault is still there, the monitor can turn unhealthy again straight away.

Diagnostics and recoveries are workflows the management pack author attached to a monitor: a diagnostic gathers information, a recovery tries to correct the fault. They are reached from the Health Explorer ("6.3 Reading the Health Explorer") and, like alert actions, need the Operator profile or better over the object.

> **Caution — A recovery changes the monitored system**
>
> A recovery runs code on the target — restarting a service, clearing a queue. Know what it does before you run it.

6 Discovered Inventory and the Health Explorer

An alert tells you something happened. The object tells you what state the thing is in now. This chapter covers finding objects in the discovered inventory and reading their health.

6.1 Browsing the discovered inventory

Open **Discovered Inventory** in the sidebar, or `/Pulse/Objects`.

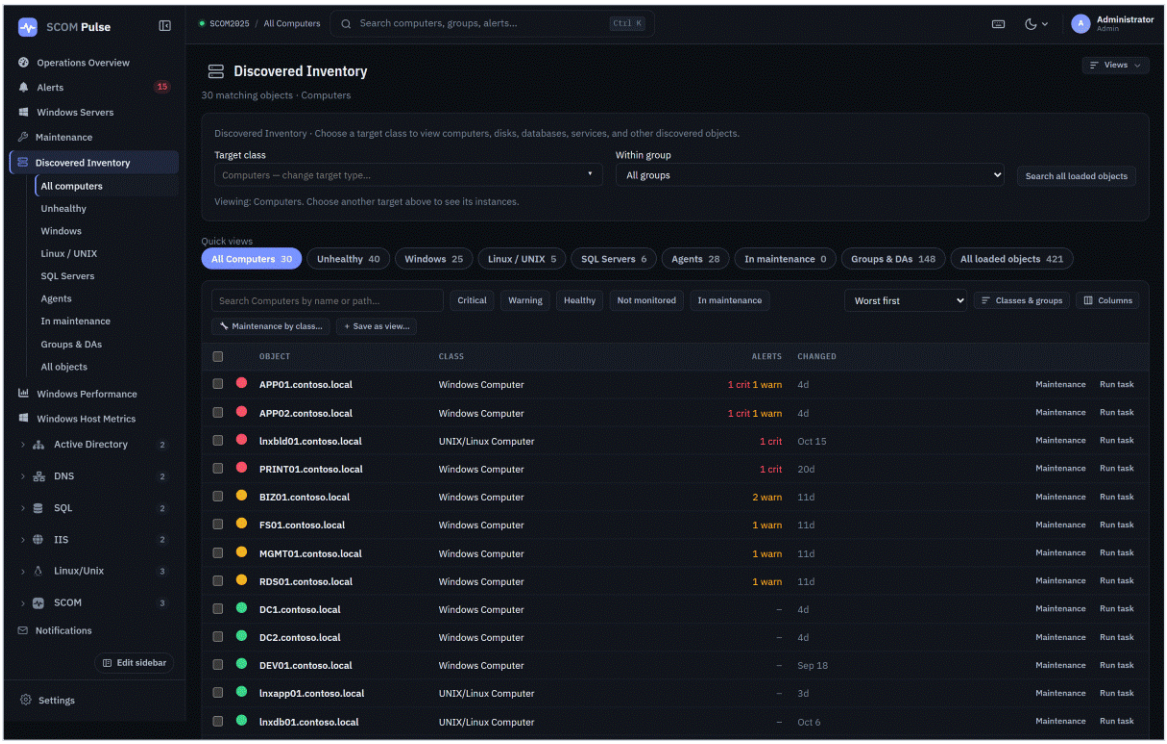


Figure 14 Discovered Inventory: choose a target class and a group at the top, pick a quick view, then narrow the grid with the state filters.

The page starts from one question: what kind of object do you want to see? **Target class** answers it. It opens on the most common loaded classes with their instance counts, and typing searches every SCOM class — computers, logical disks, databases, services — marking any class whose instances Pulse has not loaded yet. **Within group** narrows the target to the members of one group, and **Search all loaded objects** drops the class and searches everything Pulse holds.

Below that, **Quick views** are one-click scopes with live counts: **All Computers**, **Unhealthy**, **Windows**, **Linux / UNIX**, **SQL Servers**, **Agents**, **In maintenance**, **Groups & DAs** and **All loaded objects**. Above the grid, state chips (**Critical**, **Warning**, **Healthy**, **Not monitored**, **In maintenance**) narrow further, and the sort offers **Worst first**, **Most alerts**, **Name** and **Recently changed**. The search box and the line under the title always name the target you are viewing, so an empty result tells you where Pulse looked.

Classes & groups opens the full class and group directory beside the grid. **Columns** chooses what the grid shows, **Views** saves a scope you use often, and **Maintenance by class…** starts a maintenance window for every instance of a class. A group's own class has exactly one instance, the group itself, so to see what a group contains use **View members** on its row or pick the group under **Within group**.

> **Note — Inheritance versus exact class**
>
> Browsing by class can include derived classes or only the exact class. A scope of *Windows Computer* including derived classes picks up every Windows computer type; the exact class does not. When a count surprises you, check which of the two you asked for.

6.2 The object page

Click any object to open its page.

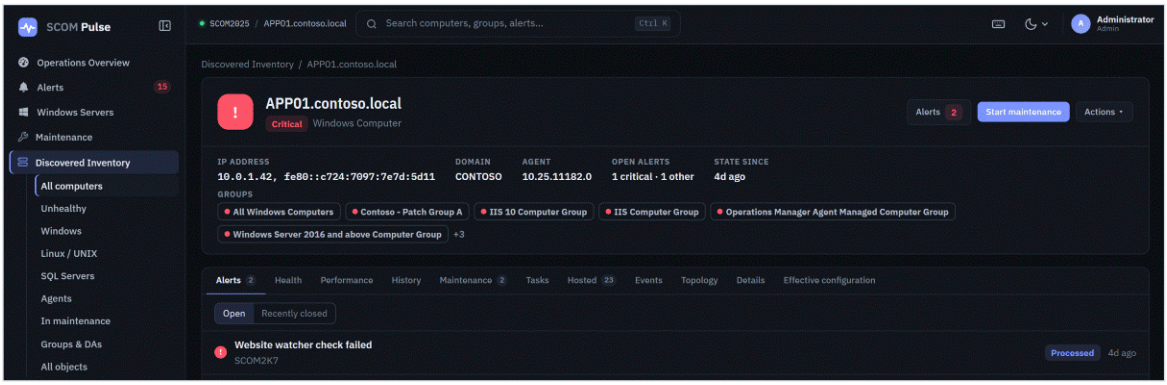


Figure 15 An object page: state, class, actions, key properties and group membership, above the tab strip.

The header carries the object's health state, its class, **Start maintenance** and **Actions** , then key properties — **IP ADDRESS**, **DOMAIN**, **AGENT**, **OPEN ALERTS**, **STATE SINCE** — and **GROUPS**.

Eleven tabs follow:

Tab	What it holds
Alerts	Open alerts on this object, with a link into the Alert Center for actions; **Recently closed** lists the ones that closed
Health	The monitor tree and the Health Explorer
Performance	Counters collected for this object
History	State changes over time
Maintenance	Windows affecting this object, past and future
Tasks	Task runs against this object, and **Run task…**
Hosted	Objects hosted on this one — the disks, databases and sites
Events	Events collected from the object
Topology	How the object relates to what is around it
Details	The full property set
Effective configuration	For administrators: every rule and monitor SCOM runs against this object, with the values in effect after overrides

Some tabs load after the page itself; a tab that is briefly empty is still loading.

Recently closed alerts. Above the alert list, **Open** and **Recently closed** switch between the alerts open now and the ones that closed — the history to read when you are troubleshooting. Choose how far back with **24 hours**, **7 days** or **30 days**, switch **Critical**, **Warning** and **Information** on or off (each shows how many closed in that period), and tick **Group by severity** to put the list under those headings. Each row names the alert, the object it was raised on, when it closed and, where SCOM recorded one, who closed it, when it was raised and how long it was open; **Show more** loads the next fifty (if alerts closed or were reopened while the list was open, a line at the end says so and offers **Refresh**), and the last row opens this object's closed alerts in the Alert Center. As on the **Alerts** tab, a computer's list includes the alerts on what it hosts. The list holds the closed alerts SCOM Pulse has on record: closure times are SCOM's where SCOM recorded one, and closed alerts are kept for the number of days set under **Settings → Sync & data → Keep closed alerts (days)** — 14 by default. When that is shorter than a period, the period is unavailable and the page says how long closed alerts are kept. The tab's count is still the open alerts.

6.3 Reading the Health Explorer

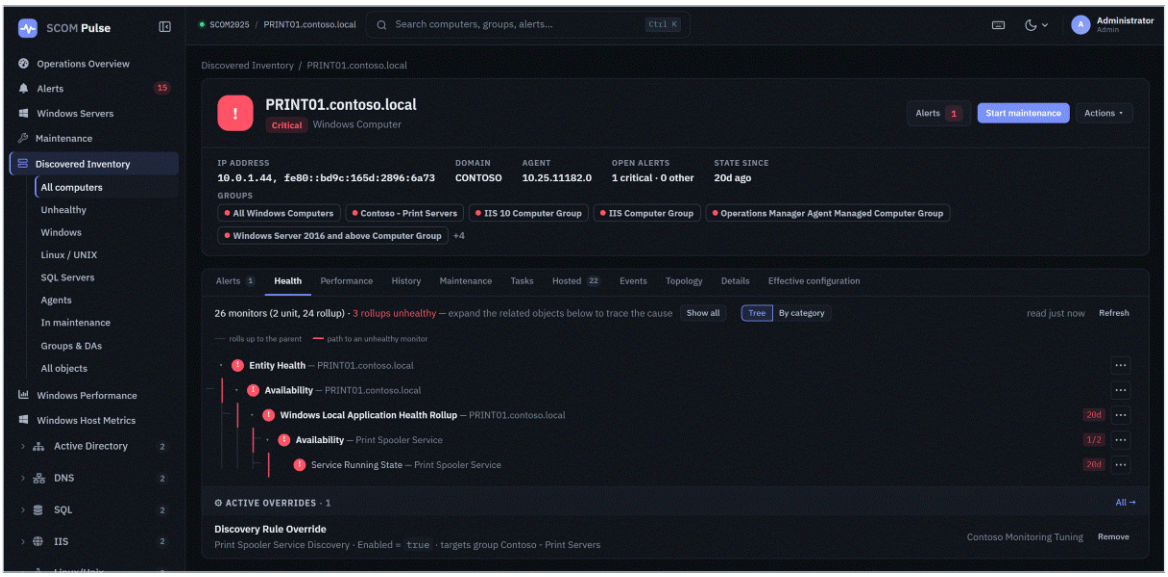


Figure 16 The **Health** tab of a Critical computer: the monitor tree under Entity Health, with the red path leading down through the rollups to the unit monitor that is actually unhealthy.

The header counts what it found — in Figure 16, "*26 monitors (2 unit, 24 rollup) · 3 rollups unhealthy*" — and offers **Tree** or **By category**, a **Refresh**, and a note of when the data was read.

Under **Entity Health** sit the four standard aspects: **Availability**, **Configuration**, **Performance** and **Security**. Each is a rollup; beneath them are the unit monitors that actually measure something. The tree marks which nodes roll up to their parent and which path leads to an unhealthy monitor, so you can walk straight down to the cause instead of expanding everything.

 ACTIVE OVERRIDES lists the overrides in force on this object, with what each changes, the class or group it targets, the management pack holding it and whether that pack is sealed. This is the first place to look when a monitor is not behaving as the management pack documents — somebody may have overridden it.

Select a monitor to see its context: what it measures, its current state, when the state last changed, and the diagnostics and recoveries attached to it.

> **Note — Why a control may be unavailable**
>
> Reset, recalculate, diagnostics and recoveries are offered only where both are true: the monitor actually has that capability, and a SCOM user role of yours with the Operator profile or better covers the object. A greyed control is usually the second of those.

6.4 History, hosted objects, events and topology

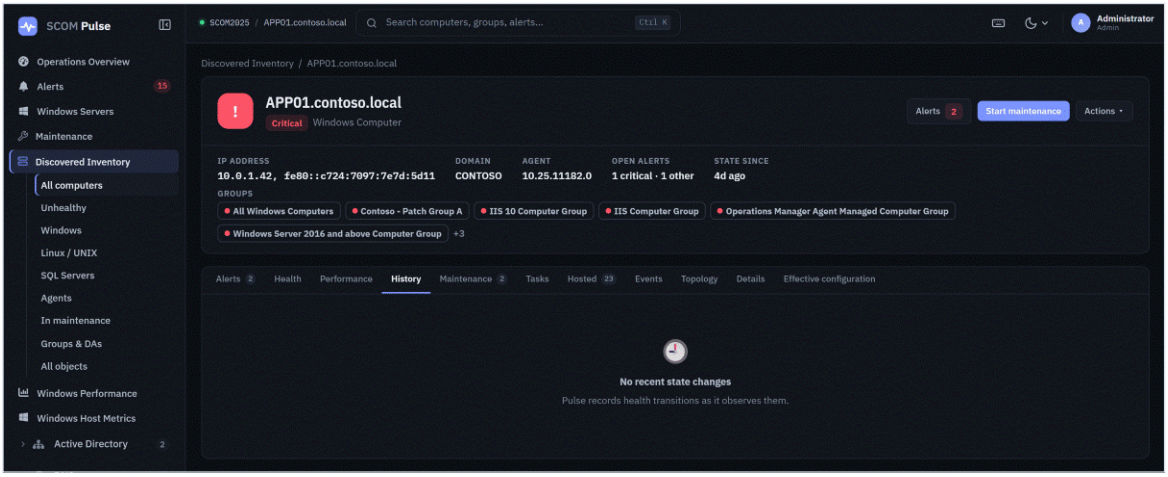


Figure 17 The **History** tab of an object whose health has not changed since Pulse began observing it. Where it has, each state change is listed with its context.

History shows state changes with their context, which is how you answer "when did this start?" — often more useful than the alert's own age. **Hosted** lists the objects this one hosts, which is how you get from a server to its disks or its SQL instances. **Events** shows collected events. **Topology** places the object among its neighbours.

6.5 Effective configuration

The **Effective configuration** tab answers "how is this server actually being monitored?" — every rule and monitor SCOM runs against the object, whether each one is enabled, whether it raises an alert and at what severity, and the parameter values in effect once every override has been resolved. The console has no such view; its only equivalent is the `Export-SCOMEffectiveMonitoringConfiguration` PowerShell cmdlet. Everything here is *configuration*: **Disabled** means disabled by configuration, not that an agent was seen not running it, and an alert severity is what the workflow would raise, not the object's current health.

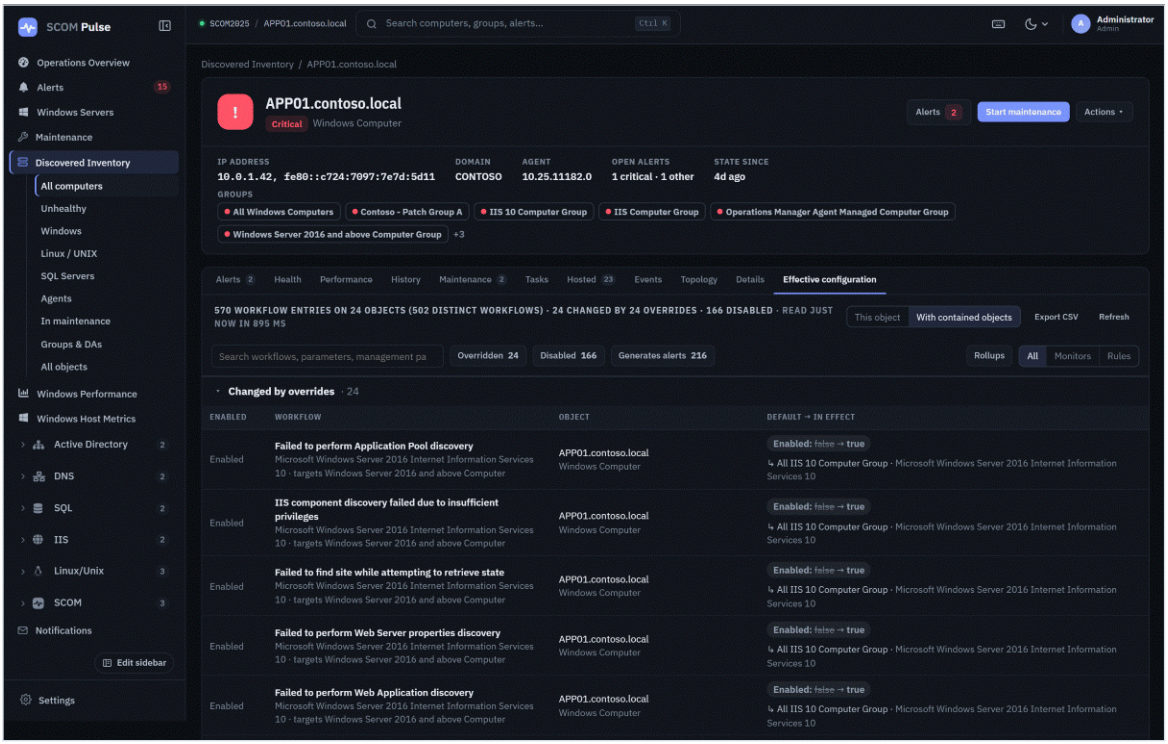


Figure 18 The **Effective configuration** tab of APP01 with its contained objects: the counts in the header, the filters, and the workflows overrides change listed first, each with its default, the value in effect and where the override applies.

Nothing is read until you open the tab. The header then says how much was found — in Figure 18, "*568 workflow entries on 22 objects (500 distinct workflows) · 24 changed by 24 overrides · 166 disabled · read just now in 1.6 s*". An **entry** is one workflow on one object: a rule that targets five databases counts five times, which is why entries outnumber distinct workflows. *Changed by* counts the entries at least one override applies to, then the override definitions responsible.

- **This object / With contained objects** chooses the scope: the object alone, or the object and everything it hosts or contains — the disks, network adapters, services, databases and sites of a server.
- **Changed by overrides** comes first, because it is usually the question: each workflow an override touches, the object it applies to, the default and the value in effect (*Threshold: ~~90~~ → 75*, *Enabled: ~~false~~ → true*), and under it where the override applies and the management pack holding it — *All IIS 10 Computer Group · Microsoft Windows Server 2016 Internet Information Services 10*, *Everything in IIS 10 Computer Group*, or *This object only*. Select that line for the override's own

name, with a **Copy** button, and whether its pack is sealed. An override that restates the default is listed too, marked *same as default*.

- Below that, one section per object. The **Enabled** column reads *Enabled* or *Disabled*; pointing at *Disabled* says why — disabled in the management pack, by an override, or because it belongs to a monitoring level the management group does not run. Disabled rows stay fully readable, since they are often what you came to find. **Alert it raises** gives the severity and priority the workflow is configured with. Parameters appear as small labels; the ones an override sets are highlighted, and pointing at one says where that override applies.
- **Overridden**, **Disabled** and **Generates alerts** filter the list, as do the search box (workflow, parameter, value, management pack or override name) and **Monitors / Rules**. **Rollups** adds the aggregate and dependency monitors, which only roll health up and have no settings of their own.
- **Export CSV** saves what is listed, one row per parameter, for Excel. **Refresh** reads it again from SCOM.

With direct SQL reads on, the tab normally fills in within a second or two. Without them the read takes several seconds per object, reaches only one level of contained objects, and cannot say which override is responsible — the tab says so when its view is limited.

7 Performance

Pulse charts the performance counters SCOM already collects. It does not collect anything itself, and it is not a reporting engine.

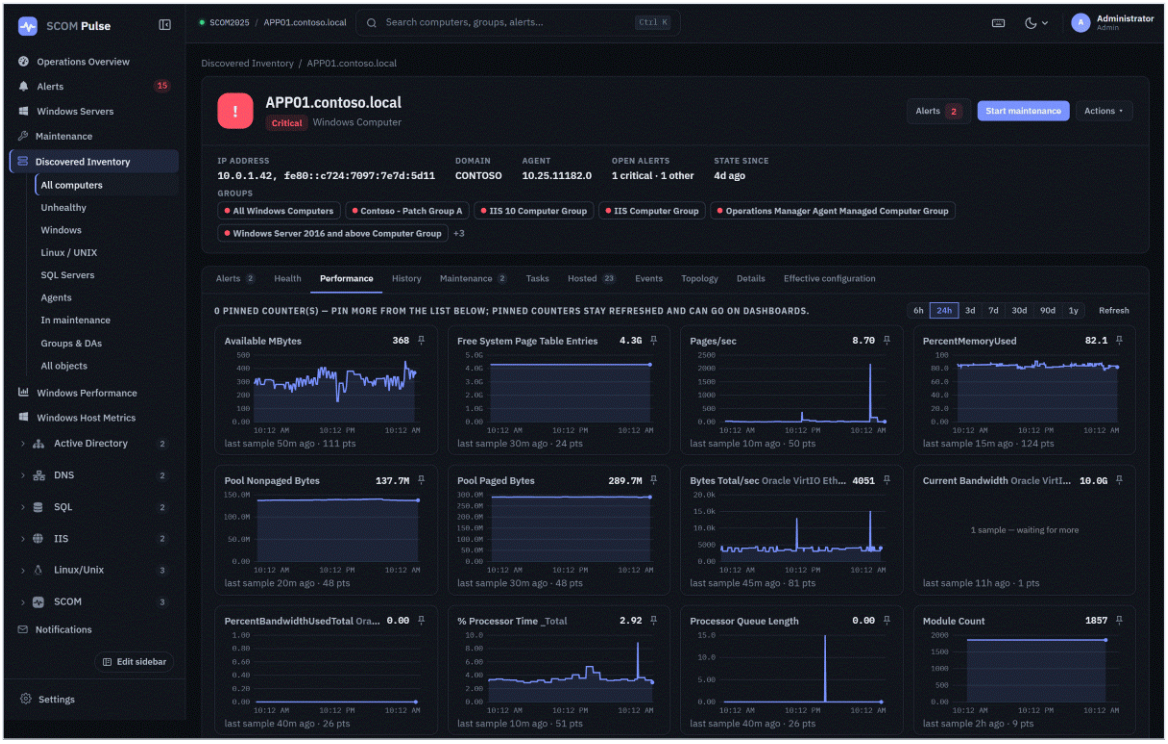


Figure 19 The **Performance** tab of an object: a chart for each counter SCOM collects for it, with the chart range above.

7.1 Choosing counters and a range

Open an object's **Performance** tab, choose one or more counters, and set the chart window. The default window in the reviewed deployment is 24 hours.

Each chart says when its counter was last sampled. Pulse keeps a counter refreshed while somebody is looking at it, or while it is pinned; a counter nobody has looked at for a while is left alone, so a chart you open after some hours shows its old line blurred, with a shimmer across it and an **Updating from SCOM…** label saying how old those samples are, and redraws sharp a few seconds later with the latest ones. A chart whose samples are current draws straight away, with no loading state.

A sparse or flat line is usually the collection rule, not a fault. Most Windows collection rules are *optimised*: the agent samples every few minutes but stores a value only when it has moved by a tolerance, and at most an hour apart, so an idle server's CPU may store one point an hour. The full-size chart's caption reads the rule — *collected every 5 min · stored when it moves ≥ 5 or after 1 h* — and names any override on those settings; on a Performance tile the same text appears when you hover the line under the chart.

Longer ranges — 30 days, 90 days, a year — are served from the SCOM **data warehouse** and appear only when the warehouse is enabled and reachable. If your administrator has not enabled it, or the check is not green, the long ranges are not offered. That is configuration, not a fault.

7.2 Why a chart can be empty

An empty chart is a real answer, and usually one of these:

- **Nothing is collecting.** The counter belongs to a rule that is disabled, or the management pack that would collect it is not installed. Check **Rules & monitors** for the collection rule and whether it is enabled ("10 Rules, monitors, discoveries and overrides").
- **Not enough time has passed.** A newly enabled collection rule produces nothing until the agent has run it and the data has arrived.
- **The object does not have that counter.** Not every object has a chart; performance is collected per class, and many classes have none.
- **The range needs the warehouse.** Short ranges come from recent data; long ranges need warehouse access.

> **Important — An empty chart is not a zero**
>
> A chart with no series is telling you that nothing was measured. That is different from a measured value of zero, and the two must not be reported as the same thing.

7.3 Pinned charts, host metrics and workload dashboards

Charts you rely on can be pinned so they refresh on a schedule and appear on dashboards. The sidebar's **Windows Performance**, **Windows Host Metrics** and workload folders are dashboards built from these cards; they are only as useful as the management packs feeding them.

8 Maintenance

Putting an object into maintenance mode tells SCOM to stop alerting on it for a period. Pulse uses SCOM's own maintenance schedules, so a window you create here is visible in the Operations console and vice versa.

8.1 The Maintenance page

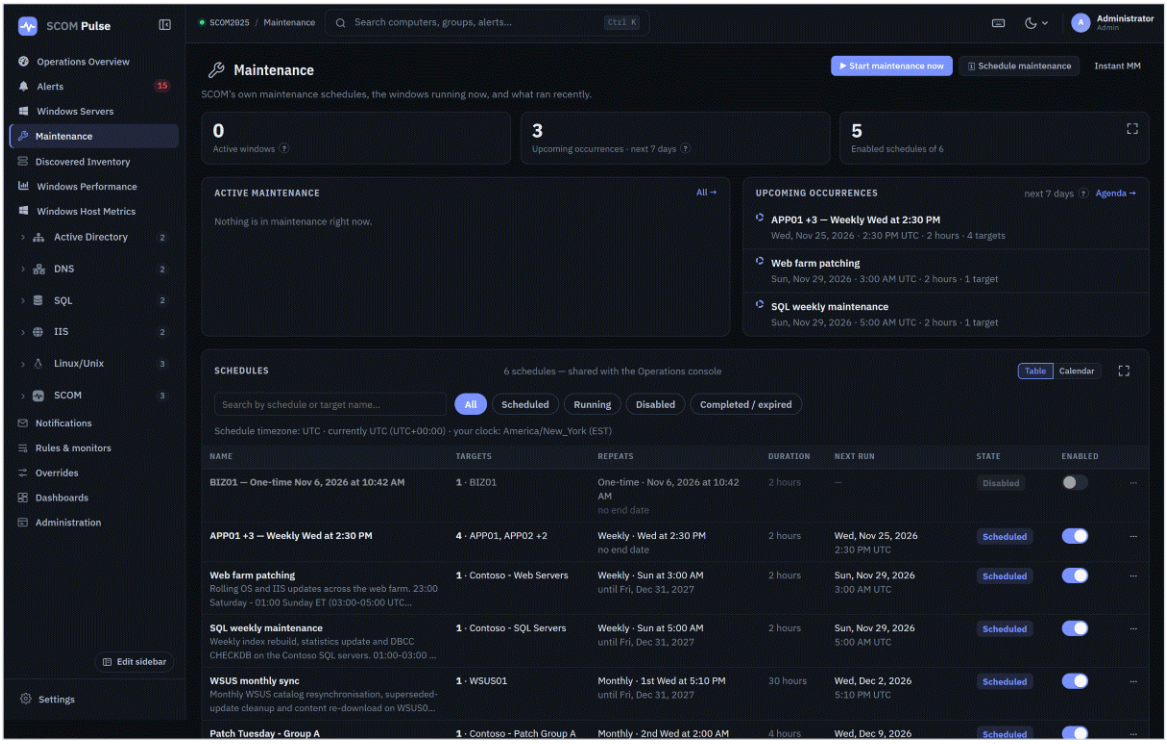


Figure 20 The Maintenance page: the counters, what is active now, what is coming in the next seven days, and the schedule table.

Across the top: **Start maintenance now**, **Schedule maintenance** and **Instant MM**. Then three counters — **Active windows**, **Upcoming occurrences · next 7 days** and **Enabled schedules**. Each counter is also a link to its section; the address it leaves in the browser (for example `/Pulse/Maintenance#schedCard`) can be bookmarked to open the page at the schedules.

Four sections follow:

- **ACTIVE MAINTENANCE** — what is suppressed right now. The card lists the first five windows, computers and groups before the objects they contain, and says how many there are in all — "*5 of 183 shown*". **Show more** lists up to a hundred, and **Show the first 5** folds it again; **All** → opens every object in maintenance as a list. Until you ask for more, the card is five windows tall however many objects are in maintenance, so the schedules below it stay where they are.
- **UPCOMING OCCURRENCES** — a projection of the next seven days, with **Agenda** →.
- **SCHEDULES** — the schedule list, in **Table** or **Calendar**, filtered by **All**, **Scheduled**, **Running**, **Disabled** or **Completed / expired**. The full screen button at the right of its heading — or the one beside the **Enabled schedules** counter — shows the schedules alone under the page head, with the table or calendar using the whole window, and keeps your search, filters and calendar position; the same button, **Esc** or the browser's **Back** returns to the whole page. The address it leaves (`/Pulse/Maintenance?full=schedules`) opens the schedules full screen and can be bookmarked.
- **RECENT HISTORY** — windows that have actually run, with a link to the audit trail.

Important — Read the timezone line, and read the recurrence — not the name

The schedule list and editor state the clock they use — in the deployment used for this guide "*Schedule timezone: UTC*", shown beside your own browser's clock. That is the timezone of the **service host**, and where that zone observes daylight saving, schedules follow it.

A schedule's name is free text and can be wrong: a schedule called *2AM Patch window* that actually repeats at 2:00 PM is an easy mistake to make and a hard one to spot. Always read the **REPEATS** and **NEXT RUN** columns rather than trusting the name.

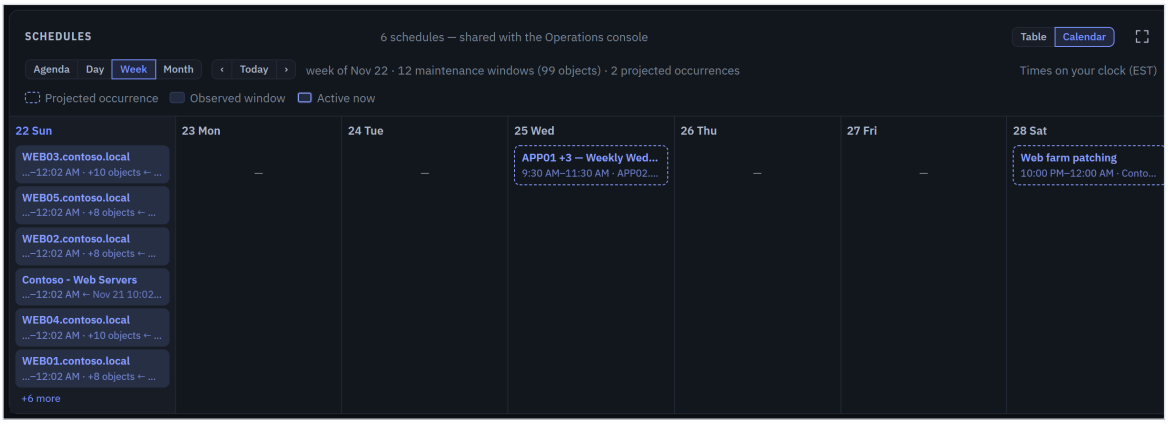


Figure 21 The schedules in **Calendar** view, a week at a time. A server that went into maintenance is one entry, with the number of objects that went with it.

8.2 Starting maintenance immediately

> **Required access — Operator profile or better, on objects your role covers**
>
> Starting maintenance suppresses alerting on real systems. The objects you may target are those covered by a SCOM user role of yours with the Operator profile or better.

Purpose — silence alerting on named objects for a fixed period, starting now.

Side effect — while a window is active, SCOM raises no alerts for those objects, and monitors do not report state. If something genuinely breaks during the window you will not hear about it.

Navigation — **Maintenance** → □ **Start maintenance now**.

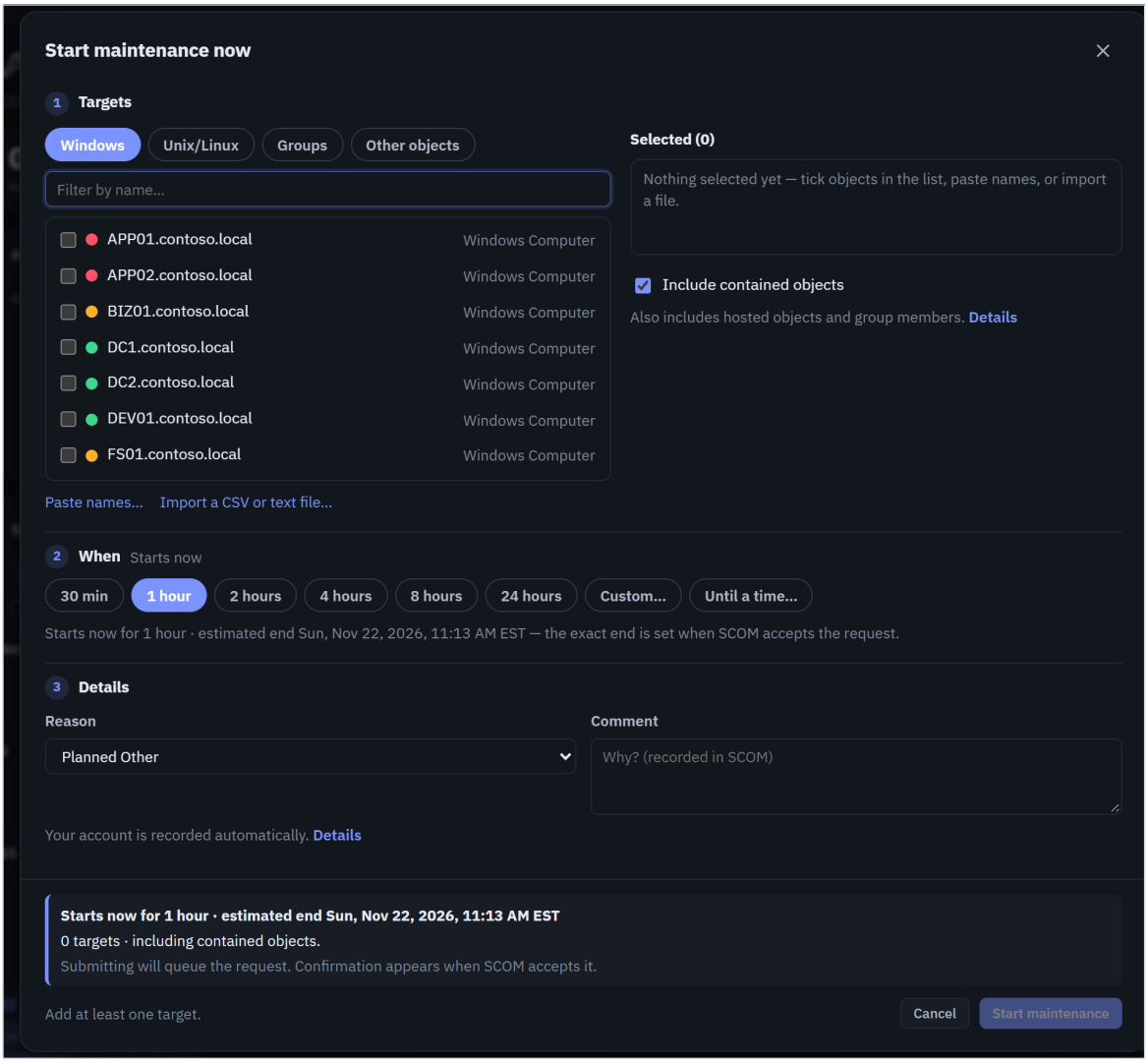


Figure 22 The **Start maintenance now** form, unsaved. The summary line and the validation message sit above the buttons.

1. In **1 Targets**, choose the objects. The tabs are **Windows**, **Unix/Linux**, **Groups** and **Other objects**. Tick them in the list, or use **Paste names...** for a list you already have, or **Import a CSV or text file...**.
2. Check **Selected (n)**. Names that could not be matched to a monitored object are reported rather than silently dropped — resolve them before you continue.
3. Decide **Include contained objects**. This extends the window to hosted objects and group members — the disks and databases on a server, the members of a group. Leaving it off suppresses the computer object alone, which is rarely what you want during patching.
4. In **2 When**, choose a duration: **30 min**, **1 hour**, **2 hours**, **4 hours**, **8 hours**, **24 hours**, **Custom...** (an amount in minutes, hours or days) or **Until a time...** (a date and time). The form states the estimated end, noting that the exact end is set when SCOM accepts the request. A window can last up to 730 days — two years, the Operations console's own limit; for one longer than 30 days the form also says, highlighted, how long it is. With **Until a time...** the window ends at exactly the time you enter, which must be between 5 minutes and 730 days from now.
5. In **3 Details**, choose a **Reason** from SCOM's list — **Planned Other**, **Unplanned Other**, **Planned Hardware Maintenance**, **Planned Application Maintenance**, **Security Issue**, **Loss Of Network Connectivity** and the rest — and add a **Comment**. Your account is recorded automatically.
6. Read the summary line, then click **Start maintenance**.

Expected result — the request is queued; "*Submitting will queue the request. Confirmation appears when SCOM accepts it.*" Once accepted, the objects appear under **ACTIVE MAINTENANCE** and the **Active windows** counter increases.

The same duration choices appear wherever you start maintenance: **Start maintenance** on an object's page, **Maintenance mode...** in the alert and object grids and their selections, a whole class, and **Instant MM**.

If it fails — **Add at least one target.** means nothing is selected. A target that resolves to no monitored object is reported in step 2. If the whole request is refused, no SCOM user role of yours with the Operator profile or better covers those objects. If the request is still waiting when the end time you chose with **Until a time...** arrives, it fails and nothing changes in SCOM; start it again with a new end.

8.3 Scheduling maintenance

> **Required access — Operator profile or better, on objects your role covers**

Navigation — **Maintenance** → □ **Schedule maintenance**.

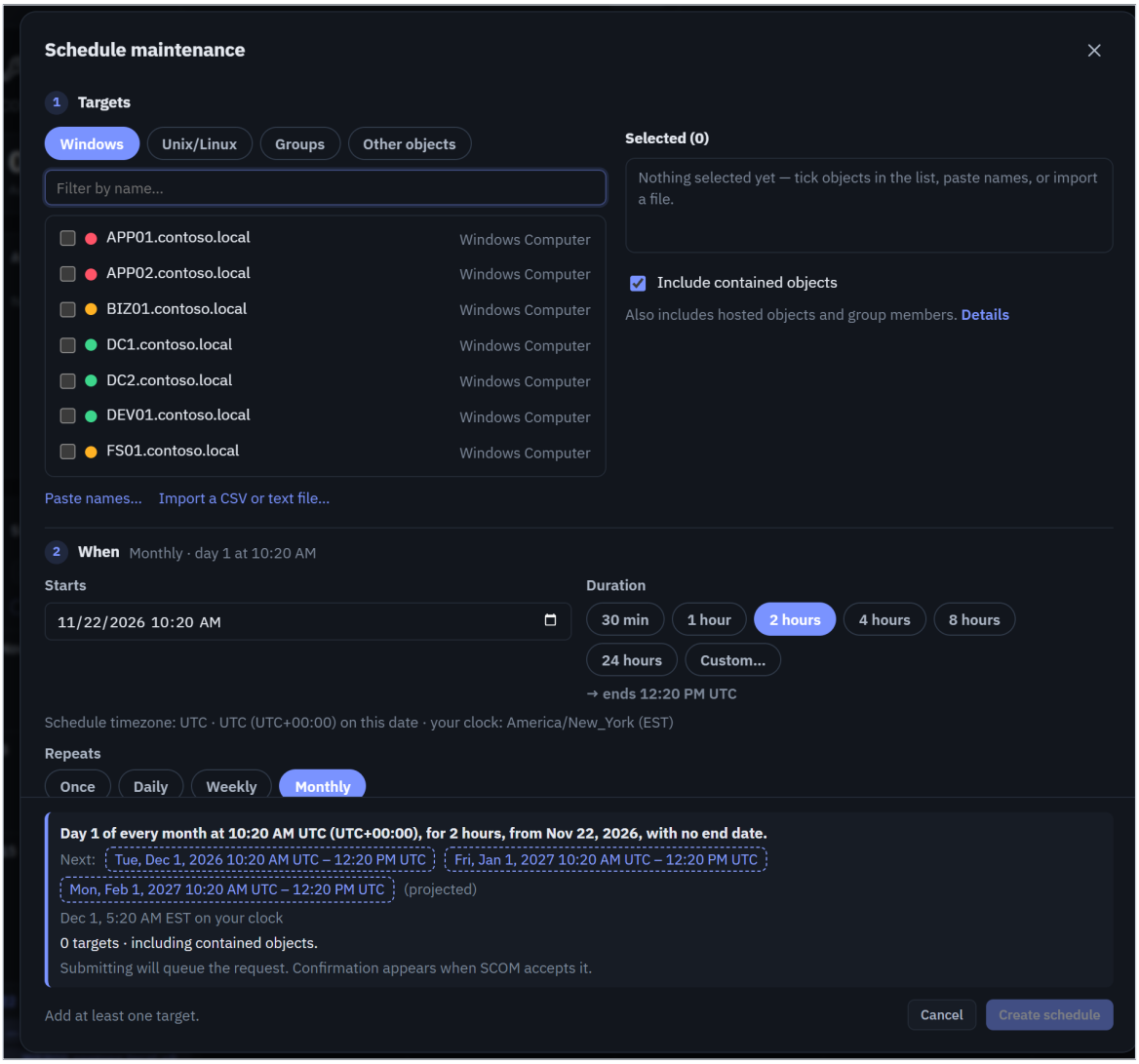


Figure 23 The **Schedule maintenance** form, unsaved, with **Repeats** set to **Monthly**.

The **1 Targets** step is identical to the immediate form. **2 When** differs:

- a start date and time, a **Duration** of up to 730 days — two years, the Operations console's own limit — and a derived end ("→ *ends 8:55 AM EDT*", with the date when it falls on a later day);
- the timezone line, which states which zone the times are in and whether daylight saving currently applies on that date;
- **Repeats** — **Once**, **Daily**, **Weekly** or **Monthly**.

In **3 Details** give the schedule a **Name**, a **Reason**, a **Comment**, and decide **Enabled** — "*Run this schedule automatically*". A schedule created with **Enabled** off exists but never runs, which is a reasonable way to stage a window before agreeing it.

Read the plain-language summary before submitting: "*Once on Fri, Sep 11, 2026, 6:55 AM – 8:55 AM Eastern Daylight Time (UTC-04:00), 2 hours.*" That sentence, not the fields above it, is what you are agreeing to.

8.4 Extending, stopping, editing and deleting

Each row's ⋯ menu holds the per-schedule actions: edit, enable or disable, and delete. An active window can be extended or stopped early. Stopping a window that was started with contained objects ends it for those objects too.

To change when an active window ends, use **Extend…** — on the object's page, in **ACTIVE MAINTENANCE**, on the calendar, on the Instant MM page, or **Extend window…** for a running schedule. **Extend by** offers **30 min** to **24 hours**, **Custom…** and **Until a time…**. A duration is added to the window's current planned end (to now, when that end has already passed); **Until a time…** sets the new end directly. The dialog shows the new end and how much later it is, and warns when your choice ends the window earlier than planned. The new end can be up to 730 days — two years, the Operations console's own limit — from now, however far off the current end is. A window that already ends later than that (one set by a script, say) can still be ended, or brought inside the limit with **Until a time…**; adding time to it is refused with the reason. Extending a running schedule's window leaves the schedule's own duration and its future occurrences unchanged.

8.5 Verifying that maintenance actually ran

> **Caution — An upcoming occurrence is a projection, not evidence**
>
> **UPCOMING OCCURRENCES** computes what *should* happen from the recurrence. It is not proof that anything ran. A schedule that exists and has never run shows exactly that combination: an upcoming occurrence beside a **RECENT HISTORY** that reads "*No maintenance history yet*".

To confirm a window ran:

1. Look at **RECENT HISTORY** on the Maintenance page.
2. Open an affected object and check its **Maintenance** tab.
3. Follow **Audit trail** → for the request, who submitted it and what SCOM reported per target.

8.6 Instant MM

Instant MM is a small page for putting a single computer into maintenance quickly, linked from the Maintenance page at `/Pulse/Maintenance/InstantMM`. It tries to identify the computer you are on and otherwise offers a search. It offers the same duration choices as **Start maintenance now**, including **Custom…** and **Until a time…**, for a window of up to 730 days — two years, the Operations console's own limit — and **Extend or change the end…** once the computer is in maintenance.

There is also a separate URL endpoint intended for scripts and task sequences. It is **off by default** and is a real action even on a GET — visiting it starts or stops maintenance. In the deployment reviewed for this guide it was disabled, and the page said so: "*script endpoint disabled on this server.*"

> **Caution — Never open the Instant MM API endpoint to see what it does**
>
> The endpoint acts when it is called. If your administrator has enabled it, use it only from the automation it was meant for, with the correct `/Pulse` prefix, and treat its response as meaningful: **200** means the request completed, **202** means it is still queued or running. Anything else has not taken effect.

9 Tasks

A SCOM task is a piece of work the agent runs on a monitored system — pinging a host, restarting a service, listing processes. Pulse can run the tasks that apply to an object and show you their output.

> **Required access — Operator profile or better, and the task in your role's task scope**
>
> Task permissions are separate from alert permissions: each SCOM user role carries its own task scope, and the role must cover the object as well. An account that may acknowledge alerts is not automatically allowed to run tasks.

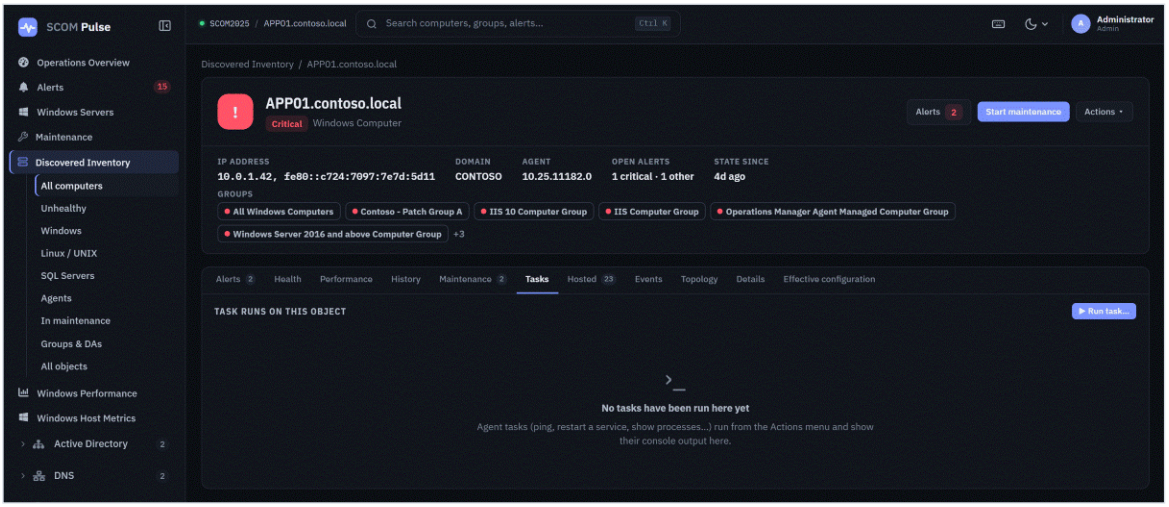


Figure 24 The **Tasks** tab of an object before anything has been run, with ▷ **Run task...**.

Navigation — open the object → **Tasks** → ▷ **Run task...**, or use **Actions** ▷ in the object header or on an alert (**NEXT STEPS** → **Run agent task**).

1. Choose a task. Only tasks whose target class matches the object are offered, grouped by category. Tasks that launch a program on **your own** machine — Remote Desktop, Computer Management, ping — are listed under **CONSOLE TASKS · RUN THESE IN THE OPERATIONS CONSOLE** and

marked *console only*: a browser cannot start them. **TASKS ON HOSTED OBJECTS** reaches the tasks that belong to the disks, databases and sites this object hosts.

2. Supply any **parameters** the task defines.
3. Choose the **Task account**:
   - **Use the task's configured account** — what SCOM would use anyway, selected from the task's Run As profile or the default Action Account.
   - **Use another account for this run** — enter **Account** (`DOMAIN\user`) and **Password**.

An option you cannot pick tells you why underneath the list. The commonest reason is transport: on a site served over plain HTTP the second option is withheld with "*Open SCOM Pulse over HTTPS to supply task credentials.*" — a password must not cross an unencrypted connection (Figure 25).

4. Confirm the targets. A task can be run against several objects at once.
5. Submit, and read the confirmation.

> **Important — A per-run password is never stored**
>
> "*Used for this run only. The password is not saved.*" It is held in the service's memory for exactly as long as the run needs it and never reaches the database — which matters because the action payload **is** the audit trail and gets exported as JSON lines. Pulse still submits the request through its own service account; the execution account is what the task runs as on the target.
>
> If the service restarts, the handle expires or the handoff fails, you are asked to enter the credentials again. Pulse never quietly falls back to the service account instead. Password-like task **parameters** remain refused, because ordinary parameters are persisted in history and audit exports.

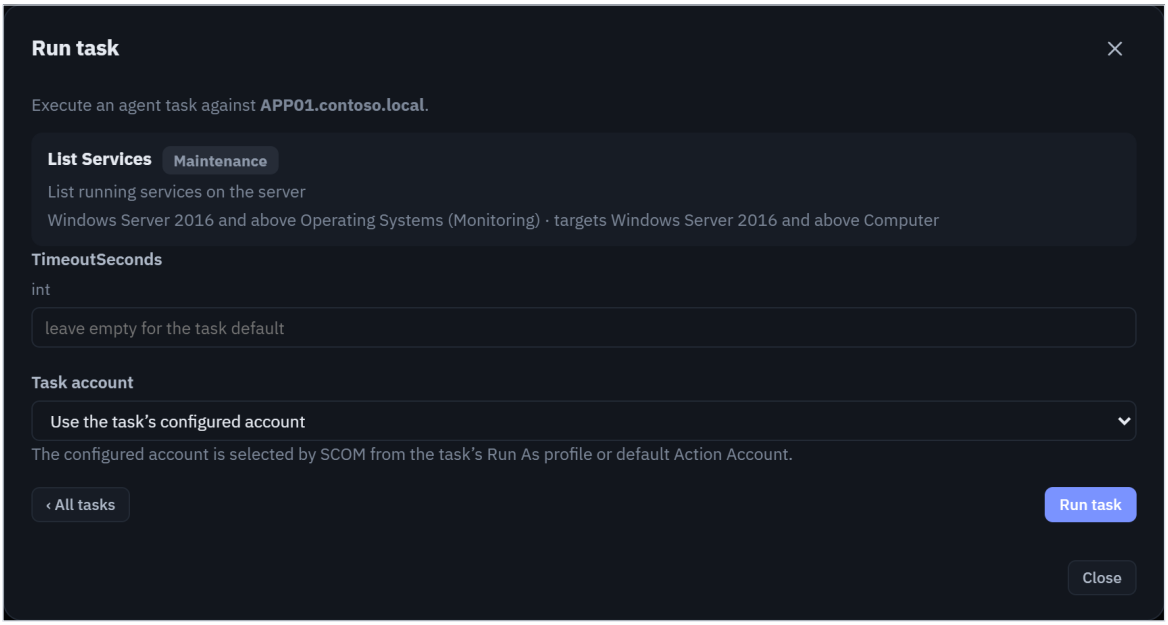


Figure 25 The **Run task** dialog with a task chosen: its parameters, and the **Task account** choice. This deployment is served over HTTPS, so nothing is withheld and the note under the list explains the selected option.

Whether you may run a task is SCOM's decision alone: one of your roles must be allowed to run tasks, list the task in its task scope, cover every target, and allow the account option you chose. A bulk run asks for a typed confirmation before it goes. So do the few agent-management tasks with wide reach — running arbitrary PowerShell, deleting an agent, installing software: they ask for an explicit confirmation (typed, for the PowerShell one) and are audited, and they no longer need the Administrator profile.

Expected result — the run appears with a state of queued, then running, then completed or failed, and its console output is shown per target on the object's **Tasks** tab. As with bulk alert actions, a multi-target run reports **per target**: some targets can succeed while others fail.

> **Important — A task runs code on the monitored system**
>
> Read what the task does before running it, particularly anything that restarts a service. Diagnostics, recoveries and tasks are three different things. All need the Operator profile or better over the object; a task must also be in your role's task scope. See "5.8 Reset health, diagnostics and recoveries".

10 Rules, monitors, discoveries and overrides

Rules & monitors is the catalogue of everything your management packs actually run. **Overrides** is the record of every place someone has changed one.

10.1 Finding a workflow

Open **Rules & monitors** in the sidebar, or `/Pulse/Workflows`.

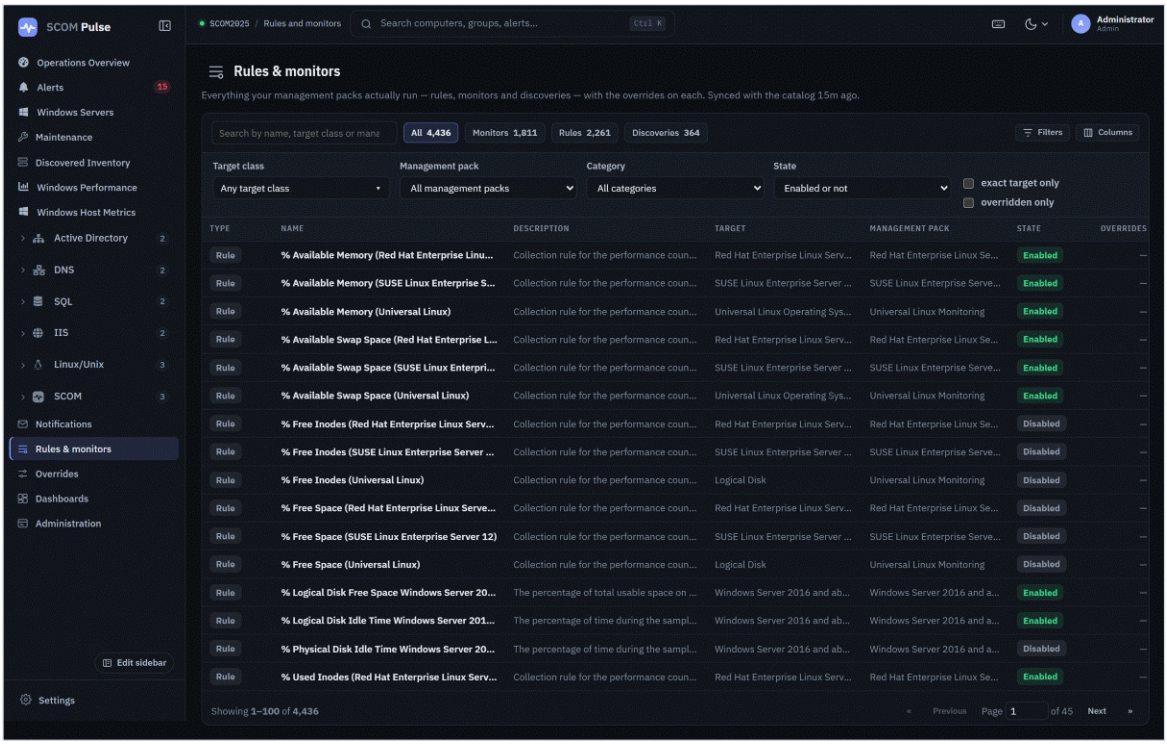


Figure 26 Rules & monitors with the filter panel open. The type counts sit above the grid.

The counts across the top split the catalogue by type — in the reviewed deployment **All 4,420**, **Monitors 1,805**, **Rules 2,261**, **Discoveries 354**. **Filters** narrows by target class, management pack, category and enabled state; **Columns** chooses what the grid shows.

The **STATE** column tells you whether a workflow is **Enabled** or **Disabled** as shipped, and **OVERRIDES** shows how many overrides touch it. Those two columns together answer the most common question an operator has about this page: *is this thing actually running here?*

10.2 Reading a workflow's properties

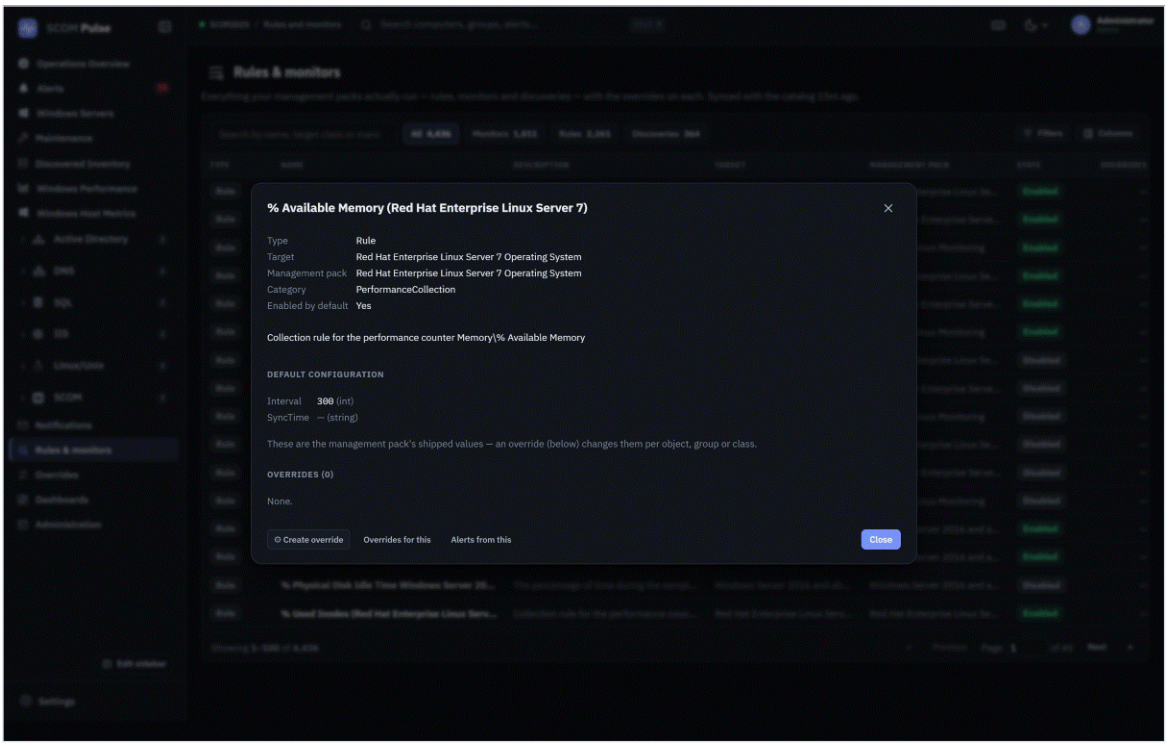


Figure 27 A workflow selected in the catalogue, with its properties and the overrides that apply to it.

Selecting a row shows what the workflow targets, which management pack defines it, its category, and the overrides in force. From there you can reach the alerts it has raised.

> **Note — Reading is not authoring**
>
> Anyone who can reach this page can read it. Creating or changing an override is a different permission — see below.

10.3 Overrides

Open **Overrides** in the sidebar, or `/Pulse/Overrides`.

The page opens on every override in the management group — in the reviewed deployment "*492 overrides across the management group*" — sorted **Unsealed first, recently changed**, and can be grouped

By rule / monitor, **By target** or **By management pack**. Each row shows what changed (**Enabled = false**), the target, the pack holding the override, when it changed and the description.

10.4 Creating an override

> **Required access — Advanced Operator profile or better**
>
> `/Pulse/Overrides` requires at least the Advanced Operator profile. With it you may override on objects and groups your role covers; an override on a whole class needs the Author profile or better.

Purpose — change how a rule or monitor behaves for a specific object, group or class: turn it off where it is noise, turn it on where the pack ships it disabled, or change a threshold.

Side effect — an override changes monitoring for everything in its scope, silently and indefinitely. An override that disables a monitor on a class disables it on every instance of that class, including ones added later.

Navigation — **Overrides** → □ **Create override**.

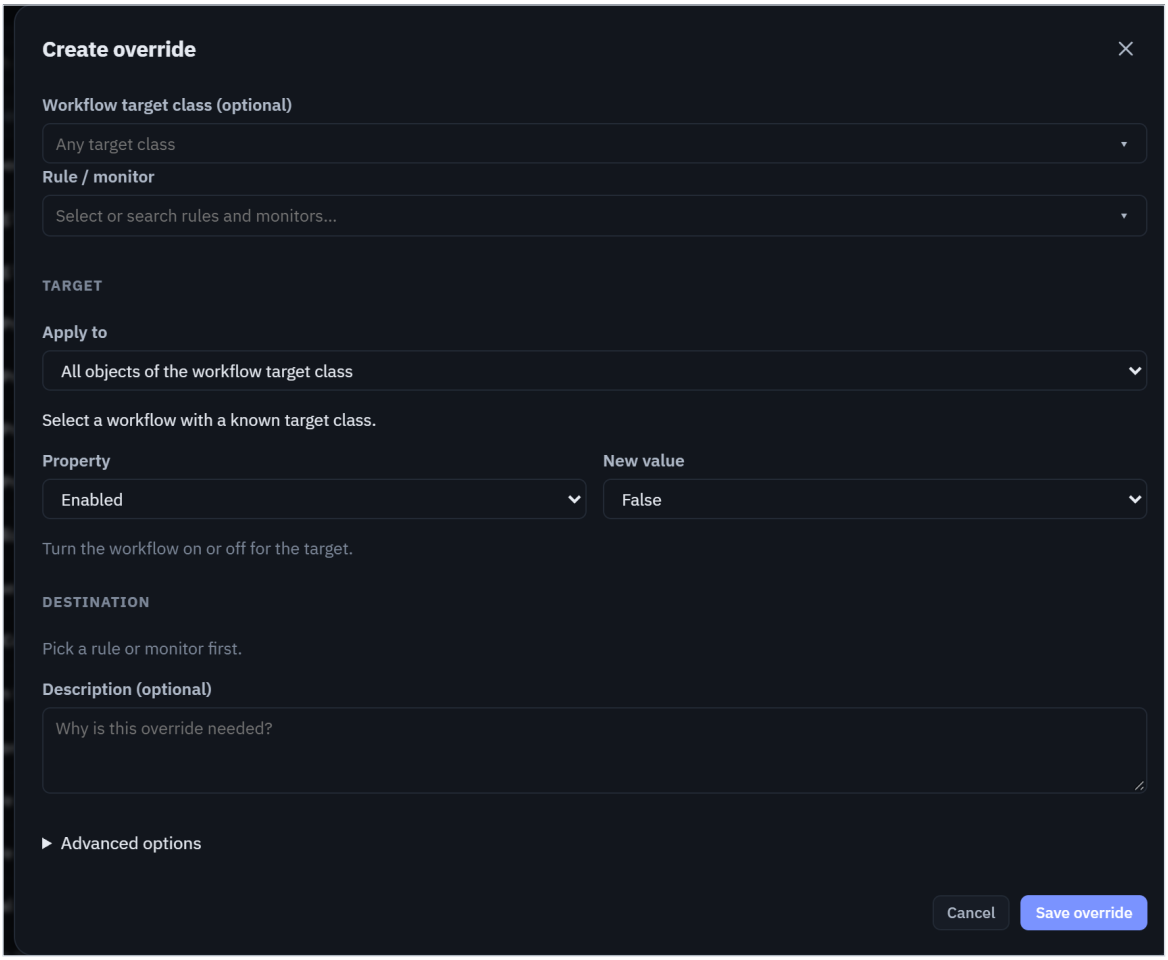


Figure 28 The **Create override** form, unsaved. The destination pack is chosen only after a rule or monitor is picked.

1. Pick the **Rule / monitor** to override.
2. Choose the **TARGET**. You may scope to a **Group**, to a single **computer / object**, or to a **class**. Narrow is safer: a single object affects one thing; a class affects everything of that kind.
3. Choose the **Property**. **Enabled** is offered directly; **Other parameter…** exposes the rest of the workflow's parameters.
4. Set the **New value** — for **Enabled**, **True** or **False**.
5. Check the **DESTINATION**. Until a rule or monitor is picked the form says "*Pick a rule or monitor first.*" Overrides must go into an **unsealed** management pack. Pulse recommends a pack only when it has a reason tied to this product — it already holds overrides for the same management pack, already

references it, or is named for the product family — and shows that reason next to **(recommended)**. When no pack qualifies the list opens on **Choose a management pack...** and nothing is chosen for you: a SCOM Administrator creates the product's own pack with **New pack...** (identity and display name are filled in from the product), and anyone can pick an existing pack under **See more — all unsealed packs**. **Save override** is refused until a destination is chosen. Pulse never recommends a shared catch-all pack, and never the Default Management Pack.

6. Give the override a **Name** and a **Description**. Write the description for the person who finds it in a year — why, and what would make it removable.
7. Decide **Enforced**, then **Save override**.

Expected result — the override appears in the list, and in the **ACTIVE OVERRIDES** section of any affected object's **Health** tab.

> **Important — Use dedicated unsealed packs**
>
> Storing overrides in a per-product unsealed pack means uninstalling that product is one pack removal. One pack for every product's overrides is the habit SCOM dropped the Default Management Pack default to stop, so Pulse does not suggest one; the Default Management Pack itself is refused outright. The company prefix that names new packs is an administrator setting; see the Administration Guide.

Editing, suspending and restoring existing overrides is done from each row's controls on the same page. Removing an override returns the workflow to whatever the management pack or a broader override says — not necessarily to "on".

11 Dashboards and your personal workspace

11.1 The dashboard library

Open **Dashboards** in the sidebar, or `/Pulse/Dashboards`.

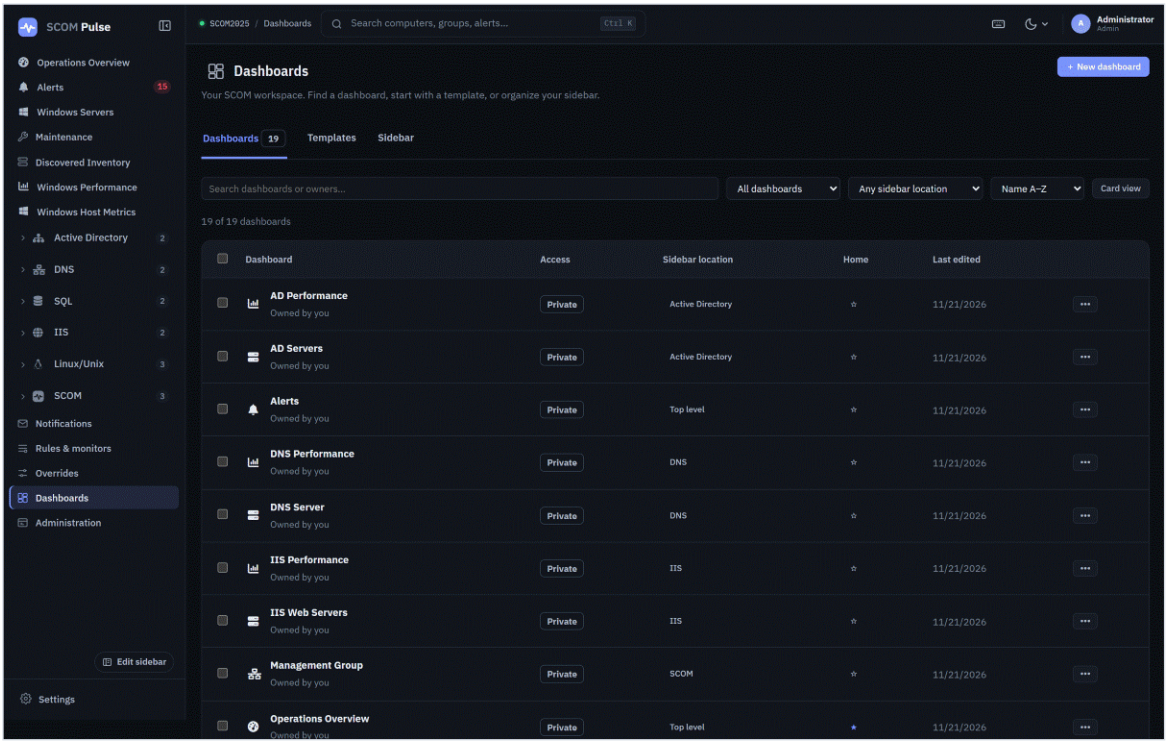


Figure 29 The dashboard library: ownership and location filters on the left, dashboards listed with their access, sidebar location and home marker.

Three tabs: **Dashboards**, **Templates** and **Sidebar**. Filters narrow by ownership (**All dashboards**, **Mine**, **Shared with me**) and by sidebar placement (**Any sidebar location**, **Shown in sidebar**, **Hidden from sidebar**, then each folder). Sort by **Name A–Z** or **Last edited**, and switch between the table and **Card view**.

The table shows each dashboard's **Access** (**Private**, or shared), its **Sidebar location**, whether it is your **Home** (the star), and when it was last edited.

> **Note — Even the built-in pages are dashboards**
>
> **Alerts** and **Operations Overview** are ordinary user-owned dashboards in the reviewed deployment. That is why your colleague's Pulse can look different from yours, and why nothing in this guide depends on a particular dashboard number.

11.2 Templates

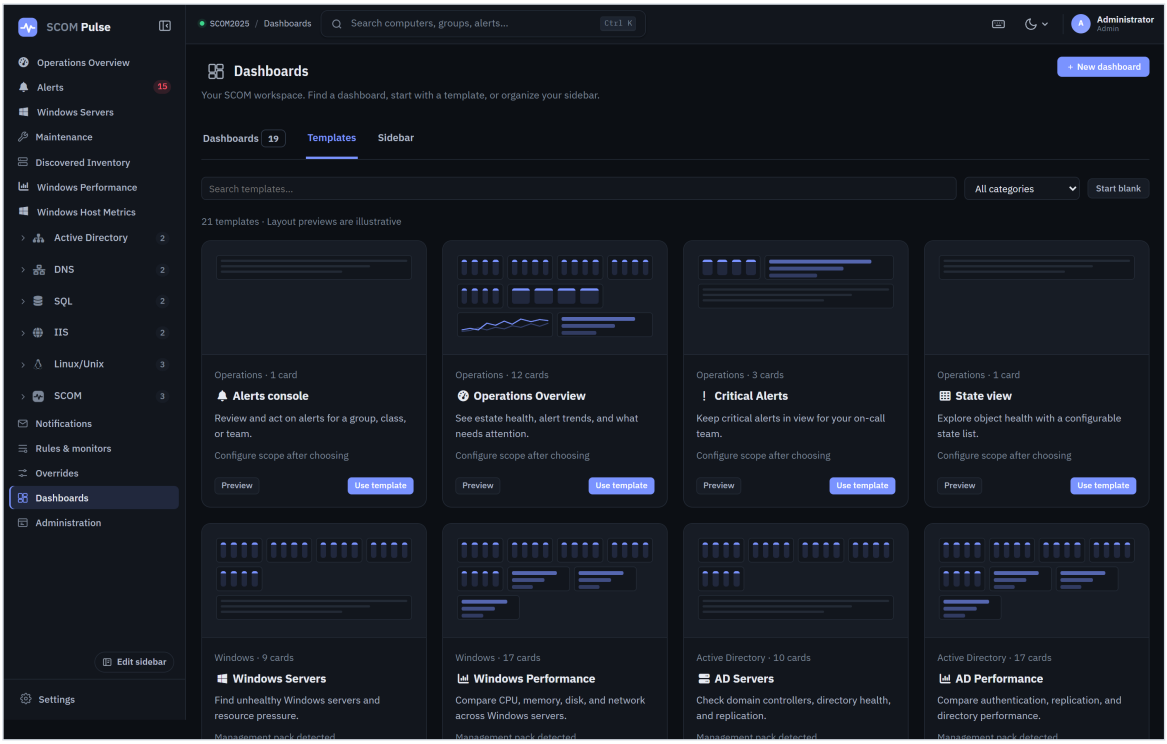


Figure 30 The **Templates** tab — starting points for a new dashboard.

Templates are starting points. Creating from a template copies it into your own dashboards; it does not link to it.

11.3 Creating and editing a dashboard

1. Click **New dashboard**, or start from a template.
2. Give it a name and an icon.
3. Use **Add card** to place cards. Card types available in the reviewed deployment include alert lists, state and health rollups for a group, unhealthy-object and degradation lists, summary and top-alert cards, pinned performance charts, noisiest-rule cards, and free-text notes. An administrator-only card can run a read-only query over the Pulse store.
4. Give each card a **scope** — the group, class or object it reports on — and a width; cards are laid out on a column grid.
5. **Save** to keep the layout, or **Cancel** to discard it.

Layout editing is an explicit mode: you enter it, change things, and save or cancel. Renaming, changing the icon, pinning to the sidebar and choosing a home dashboard are separate controls on the dashboard itself.

> **Note — Check the card list rather than assuming**
>
> Card types vary between builds. Open **Add card** and read what is offered rather than working from a list in a document.

11.4 Home, folders and the sidebar

Mark any dashboard as **Home** with its star to make it the page you land on. Folders group dashboards in the sidebar, and the **Sidebar** tab ("11.5 Organising the sidebar") is where you organise and reorder them.

11.5 Organising the sidebar

The **Sidebar** tab of the dashboard library controls what appears in your sidebar, which folder each dashboard sits in, and the order. Add a folder, drag entries between folders, then **Save** — or **Cancel** to leave the sidebar as it was.

11.6 Sharing: three different things

Open a dashboard and click its **Private** / **Shared** badge (Figure 31).

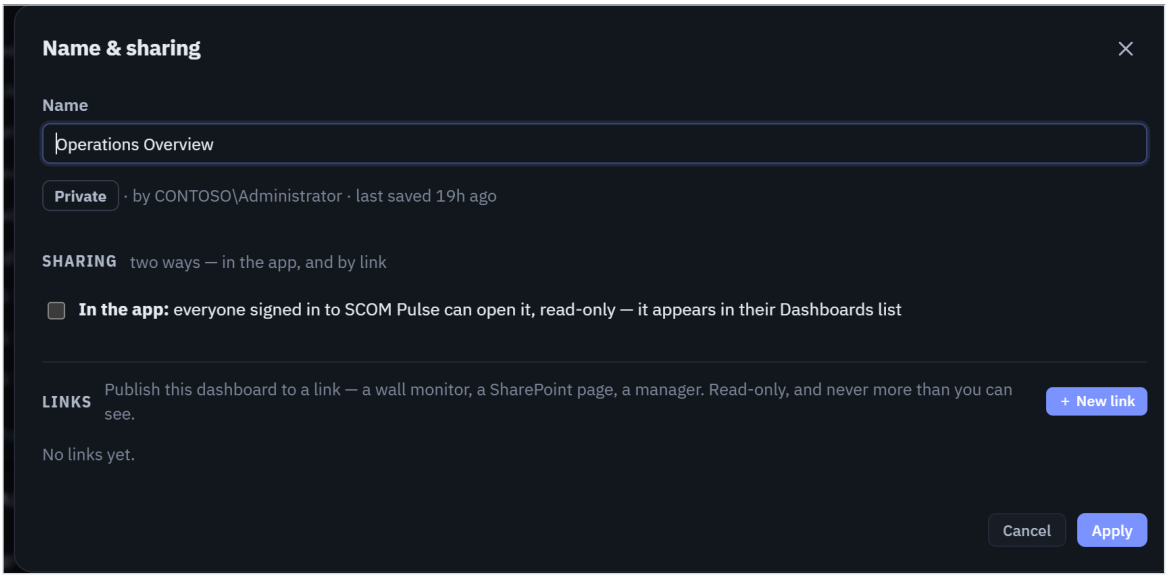


Figure 31 The **Name & sharing** dialog for a dashboard, opened from its **Private view** badge. No link was created.

Distinguish carefully:

	What it is	What the other person sees
Private	The default. A personal dashboard configuration	Nobody else sees your layout
Shared with signed-in users	Other Pulse users may open your dashboard	They sign in as themselves. They see **their own** data through your layout
Published link	A read-only URL	Whatever the **publisher** may see, re-checked on every request

> **Important — Sharing a configuration is not sharing access**
>
> Sharing a dashboard with a colleague shares the *layout*. It does not widen their alert or object permissions — whoever opens it still sees only what their own SCOM user roles allow. A **published link**, by contrast, shows the publisher's view to whoever opens it, which is why publishing is restricted and audited.

Publishing a link requires the dashboard's owner to hold the Operator profile or better (or an administrator to publish it) and the policy to be enabled. Options for audience, expiry, embedding and revocation depend on what your administrator allows; whole-management-group exposure requires explicit confirmation. Revoking a link stops it serving immediately.

Documentation gap — Published links were not exercised

No link was published while this guide was written, because publishing is a real, outward-facing change. The dialog above was opened and cancelled. Field-by-field behaviour of link creation is documented in the Administration Guide from the sharing policy and settings, and is marked unverified there.

12 Notifications

Notifications are SCOM's own channels and subscribers. Pulse lets you manage the subscriptions that notify **you**.

> **Required access — Operator profile or better, for the subscriptions that notify only you**
>
> There is no Pulse setting for this: SCOM decides. With the Operator profile or better you manage the subscriptions that notify only yourself — **My notifications** — and never channels. A role that administers notifications — the SCOM Administrator profile, or a Delegated Administrator role with **Notification Management** that is not limited to groups — manages every subscription, subscriber and channel. A Read-Only Administrator can read them all and change none. If the role that lets you manage subscriptions is limited to groups, a subscription of yours must name groups, and cannot reach beyond that role's groups.

12.1 The subscription list

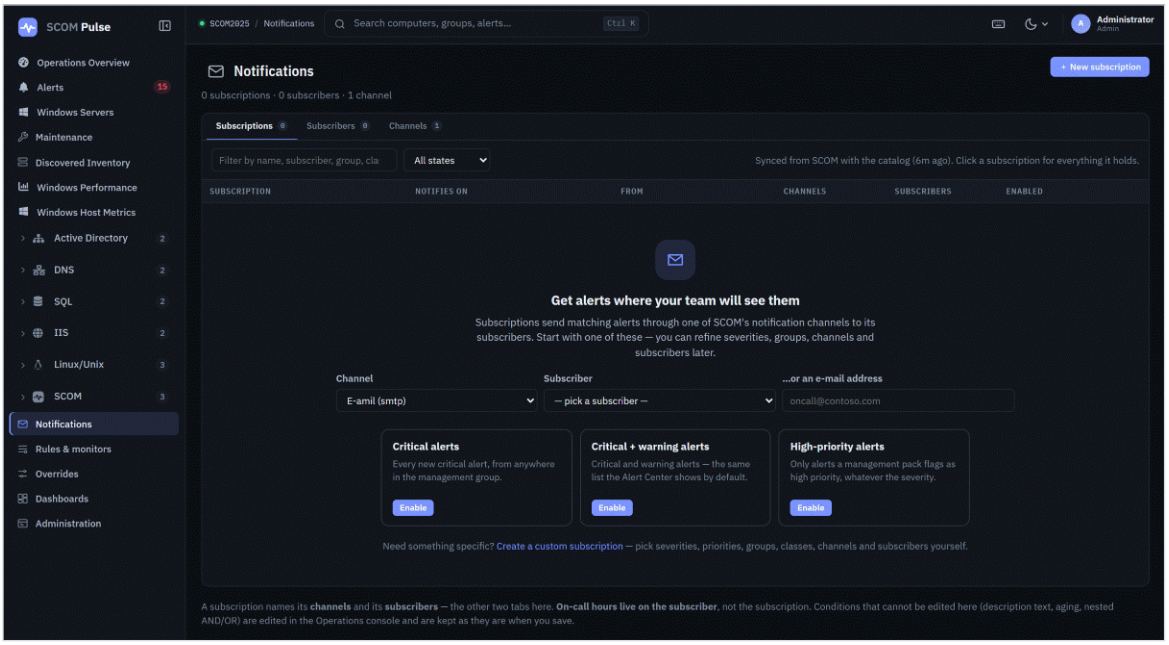


Figure 32 The Notifications page: **Subscriptions**, **Subscribers** and **Channels** as tabs. No subscription exists here yet, so the page offers three to start from.

The page has up to three tabs, each with its count: **Subscriptions**, and — for a role that reads SCOM's Administration space — **Subscribers** and **Channels**, the two lists a subscription is built from. The button

at the top right follows the tab: □ **New subscription**, □ **Add subscriber**, □ **Add channel**. With the Operator profile you see your own subscriptions and no tabs.

Each subscription is one line:

Column	What it shows
SUBSCRIPTION	Its name, and its description under it
NOTIFIES ON	The conditions an alert has to meet, as chips: the severities in their own colours, then priority, resolution state, alert-name text, rules and monitors, custom fields. What does not fit is counted — "*+2 more*"
FROM	The groups and classes it is scoped to — the first group by name, the rest counted — or *Everything in the management group*
CHANNELS	How it sends
SUBSCRIBERS	Who is notified, by name
ENABLED	The switch that pauses it

Click a row for everything the subscription holds, in the order it is read: **NOTIFIES ON** (every condition, every value), **FROM** (every group and class), **SENT TO** (the channels by name, the subscribers with their addresses) and **RECORD**; **Edit** is in its footer. The date a subscription takes effect from — *Raised after* — is there and not in the list, since the Operations console puts one on every subscription it creates.

The filter box finds a subscription by its name or description, by a subscriber, by a group or class it is scoped to, or by a channel; **All states** and **Any channel** narrow the list further.

The conditions are what SCOM Pulse can read from the subscription's criteria, one by one. Where the criteria were written in the Operations console with conditions it does not show, or nest AND and OR, the row's dialog says so, and the console shows the whole expression (12.4).

12.2 Creating a subscription

Navigation — **Notifications** → □ **New subscription**.

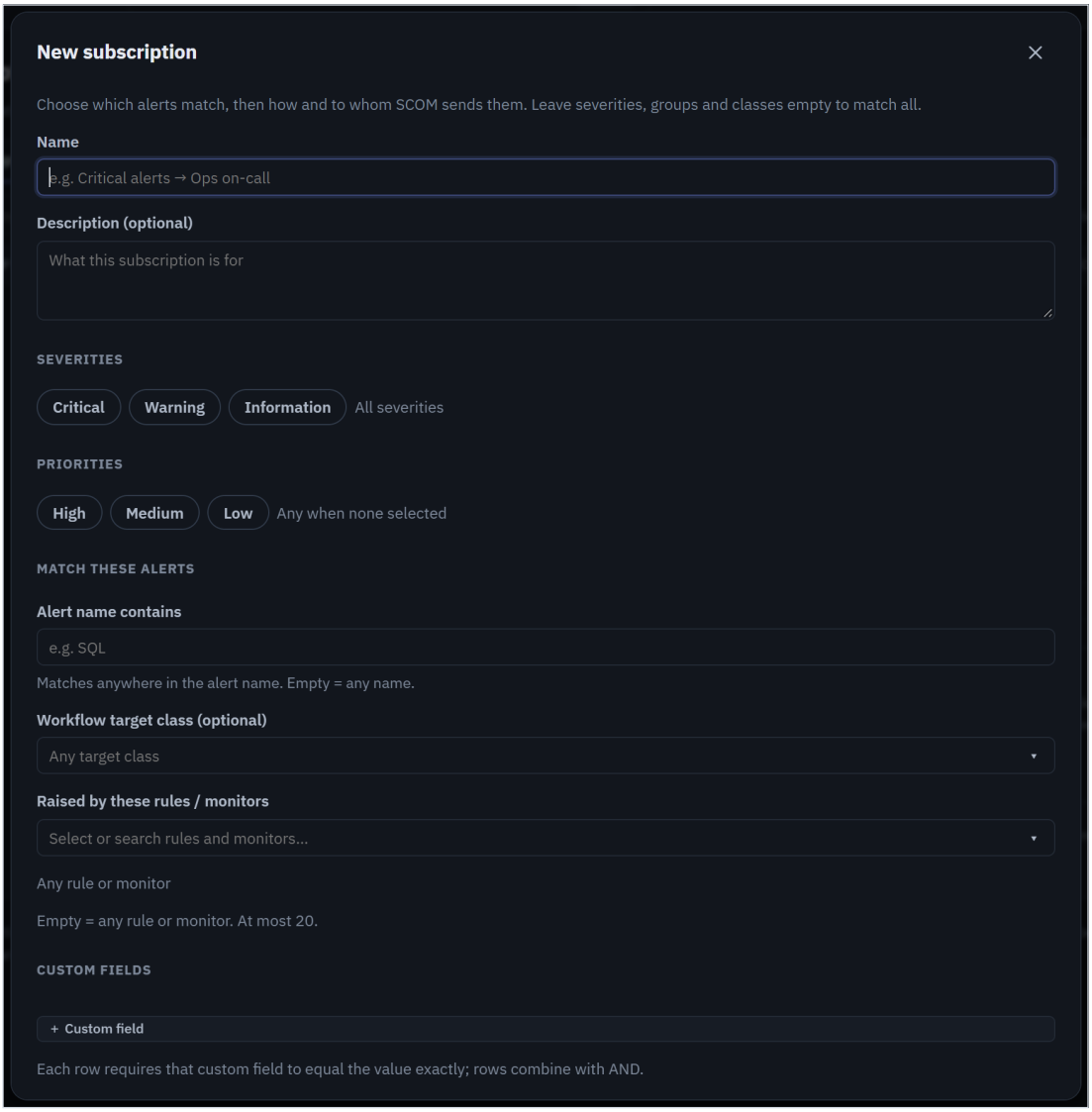


Figure 33 The **New subscription** form, unsaved, showing the criteria sections.

1. Give it a **Name** and optionally a **Description**.
2. Choose **SEVERITIES** and **PRIORITIES**. Leaving them empty matches all — the form says so: "*Any when none selected.*"
3. Narrow with **MATCH THESE ALERTS**: **Alert name contains** matches anywhere in the name; **Raised by these rules / monitors** limits to named workflows (at most 20).
4. Add **CUSTOM FIELDS** rows if you need them. Each row requires that field to equal the value exactly, and rows combine with **AND**.
5. Scope by **GROUPS** and **OBJECT CLASSES**. Empty means the whole management group and any class; classes include derived classes. If your role is limited to groups you must name groups, from the ones that role covers.
6. Pick the **CHANNELS** — how SCOM sends — and the **SUBSCRIBERS** — who receives. Channels and subscribers are created by an administrator on the **Subscribers** and **Channels** tabs of this page; operators choose from them but never see or edit them.
7. Decide whether to notify **only when the alert is new** (resolution state 0), which is the console default.
8. Set **Subscription enabled**, then **Create subscription**.

12.3 On-call hours live on the subscriber

A subscription has no schedule. Availability — when a person is actually notified — belongs to the **subscriber**, and is edited on the **Subscribers** tab. If somebody is being paged out of hours, the subscription is not where you fix it.

12.4 Criteria Pulse will not overwrite

Pulse supports severity, priority, groups, classes, alert-name-contains, rules and monitors, custom fields and only-new. SCOM can express more than that in the Operations console — text matching on descriptions, alert aging, nested AND/OR. Where a subscription uses those, Pulse shows it and **never overwrites** the expression it cannot represent. Edit those in the Operations console.

13 Troubleshooting and quick reference

13.1 I cannot sign in, or I am prompted for a password

Pulse uses Windows Authentication. A credential prompt usually means your PC has no browser policy naming the site, or you are not on the domain. Do not work around it by weakening authentication. Tell your administrator the exact address you opened: the settings that fix it for everyone are under **Settings → Access → Signing in without a password box**, and **/Pulse/Access** says the same.

13.2 I am read-only and I should not be

Open **/Pulse/Access**. The page states the decision and shows every test behind it.

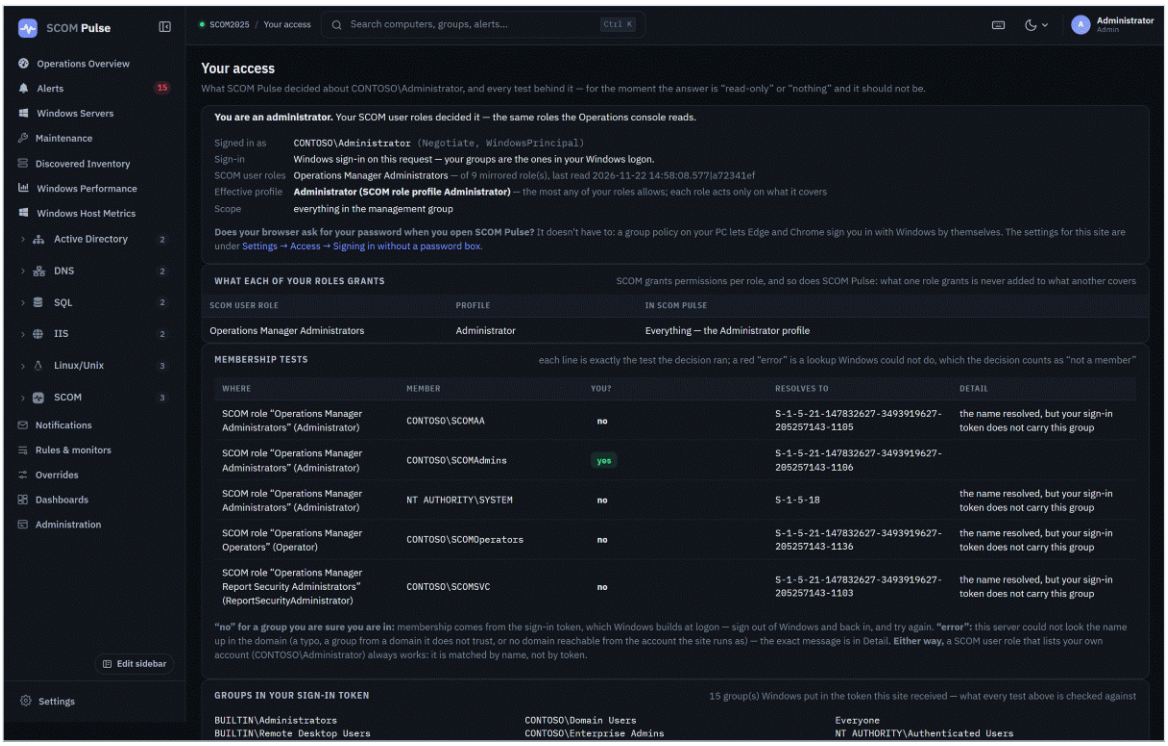


Figure 34 The **Your access** page: the decision, then what each matched role grants, then the membership tests behind it. Security identifiers are covered; the lab's account and group names are left readable.

Read it in this order:

1. The opening line — whether you are an administrator, an operator, read-only or without monitoring access, and why. Then **Signed in as**: check it is the account you expected.
2. **SCOM user roles** — the roles your sign-in matched, out of those in the management group. *none matched* is the whole answer when you see nothing.
3. **Effective profile** and **Scope** — for example *Operator (SCOM role profile Operator)*. The profile is the most any of your roles allows; each role acts only on what it covers, so a high profile here does not mean you may act everywhere you can see.
4. **What each of your roles grants** — one row per matched role, with its profile and what it grants in Pulse, and a note when that holds within the role's groups or classes only. What one role grants is never added to what another covers. A role that grants nothing says which of three things happened: *Nothing here* (the role holds no permission Pulse uses — a report role reads this way), *permissions not read* (its permission list could not be read; a custom Delegated Administrator role grants nothing until it can be), or *not readable by this SCOM client* (a profile the Pulse server cannot describe). The last two are for whoever looks after the Pulse server.
5. **MEMBERSHIP TESTS** — every member of every SCOM user role, tested against your sign-in, with **Where** it came from, the **Member**, **You?**, what it **Resolves to** and the **Detail**. **yes** means you matched. **no** with "*the name resolved, but your sign-in token does not carry this group*" means you are not in it as far as this sign-in is concerned. An **error** means the server could not look the name up at all. **not counted** marks a machine-local member such as `BUILTIN\Administrators` when the Pulse server is not a management server: the name means a group on the management server itself, and this server's own group of the same name is not what SCOM granted.
6. **GROUPS IN YOUR SIGN-IN TOKEN** — what Windows actually put in the token.

The commonest cause of an unexpected "no" is a group added after you signed in to Windows. **Sign out of Windows and back in** — closing the browser is not enough. A change to a SCOM user role itself needs no sign-out: Pulse picks it up within about a minute. Send this page to whoever is helping you; anyone can open it for themselves.

If you can see but not act, a banner says so: "*You have read-only access. Your SCOM user roles let you see this, not act on it; to take action, ask your SCOM administrator for a role with the Operator profile or better.*" If you can act in some places and are refused in another, the refusal reads "*Your SCOM user roles let you see this but not change it: no role of yours with the Operator profile or better covers it.*" — you are seeing that object through a read-only role, and your Operator role does not reach it. Either way the answer is a SCOM user role, and your **SCOM** administrator gives it.

If a banner tells you that you have no monitoring access, read which of the two it says — they need different people:

Banner	What it means	Who fixes it
"*Monitoring access is waiting for SCOM role verification. Refresh after the service synchronizes user roles.*"	Pulse has not been able to read the SCOM user roles yet. Nothing is wrong with your account	Wait for the next sync and refresh. If it persists, whoever looks after the Pulse server — the service may not be reaching SCOM
"*Your account hasn't been granted monitoring access. Ask your SCOM administrator to assign an appropriate SCOM user role.*"	You signed in successfully but hold no SCOM user role — or only a report or Application Monitoring role, which grants nothing in the monitoring views	Your **SCOM** administrator, by putting you in a SCOM user role

Both carry a **See your access details** link straight to this page. With no monitoring access you land on an **Access status** page rather than an empty dashboard; it says who you are signed in as, whether Pulse is waiting for the SCOM user roles or your account holds none, and what to ask for, with a **View my access** link to this page. An authorized person who opens that address is simply sent to their dashboard.

13.3 A number looks stale

Check the sync note on the page and the service indicator in the status bar. Different caches have different clocks. An administrator can force a refresh.

13.4 My action failed, or only partly worked

Open **My actions** in the top bar. Bulk actions report per target. Common causes: the object is outside your SCOM scope; SCOM refused to close an alert whose monitor is still unhealthy; the target no longer exists.

13.5 A chart is empty

See "7 Performance". Most often nothing is collecting, or the range needs warehouse access.

13.6 A dashboard from a management pack is missing

Workload dashboards depend on the management packs being installed and collecting. A missing SQL board on a server with no SQL management pack is correct behaviour.

13.7 A resolution state I want is not offered

An administrator can publish a shortlist of the resolution states the **Set state** menu offers, and the shortlist applies to everyone. It is a shorter menu, not a permission: anyone whose role may update alerts

may set any state the management group has. If a state you use is missing, ask a SCOM Administrator to add it to the list under **Settings**. **Closed** is always offered.

13.8 Something is not configurable here

Pulse does not reproduce the whole Operations console. Management pack authoring, distributed application design, complex group formulas, editing company knowledge, Run As credentials, network and UNIX/Linux discovery, connector configuration and SCOM reporting remain console work.

13.9 End-of-shift checklist

1. No unowned critical alerts left in the queue.
2. Every alert you worked is acknowledged or closed, with a comment and a ticket reference.
3. Any maintenance you started has an end time you are happy to hand over, or has been stopped.
4. **RECENT HISTORY** confirms that windows you expected to run actually ran.
5. **My actions** shows no failed or partly failed request you have not dealt with.
6. Anything you could not finish is written on the alert, not only in your head.

14 Glossary

Term	Meaning in SCOM Pulse
Alert	A record that SCOM raised because a rule matched or a monitor changed state
Class	The kind of a thing — *Windows Computer*, *IIS 10 Web Site*. Monitoring targets classes
Custom field 1–10	Ten free-text fields SCOM keeps on every alert, often used by connectors
Discovery	A workflow that finds instances of a class
Distributed application (DA)	A composite object built from other objects
Group	A named set of objects. Scopes permissions, overrides, notifications and dashboards
Health Explorer	The monitor tree for an object, showing which monitor makes it unhealthy
Maintenance mode	A period during which SCOM does not alert on chosen objects
Management pack	The unit in which monitoring ships. Sealed packs are read-only; unsealed packs can hold your overrides and groups
Monitor	A workflow with a health state. Its alert closes itself when it goes healthy
Override	A stored change to how a rule, monitor or discovery behaves for a scope
Pulse role	**Viewer**, **Operator** or **Admin** — Pulse's one-word summary of your SCOM profile, shown in the account chip. Nobody grants it separately: Read-Only Operator reads as Viewer; Operator, Advanced Operator and Author as Operator; Administrator as Admin
Repeat count	How many times one alert has fired
Resolution state	SCOM's workflow state for an alert, from **New** to **Closed**
Rule	A workflow with no health state. Its alert never closes itself
SCOM profile	What a SCOM user role lets its members do: Read-Only Operator, Operator, Advanced Operator, Author, Administrator. Your SCOM user roles are the whole of your access to Pulse, and each role's profile applies only to what that role covers
Smart rank	Pulse's default alert ordering, by likely importance rather than time
Unowned	An alert with no owner
Watcher	A lightweight check — website, Windows service or TCP port — that Pulse can author into SCOM