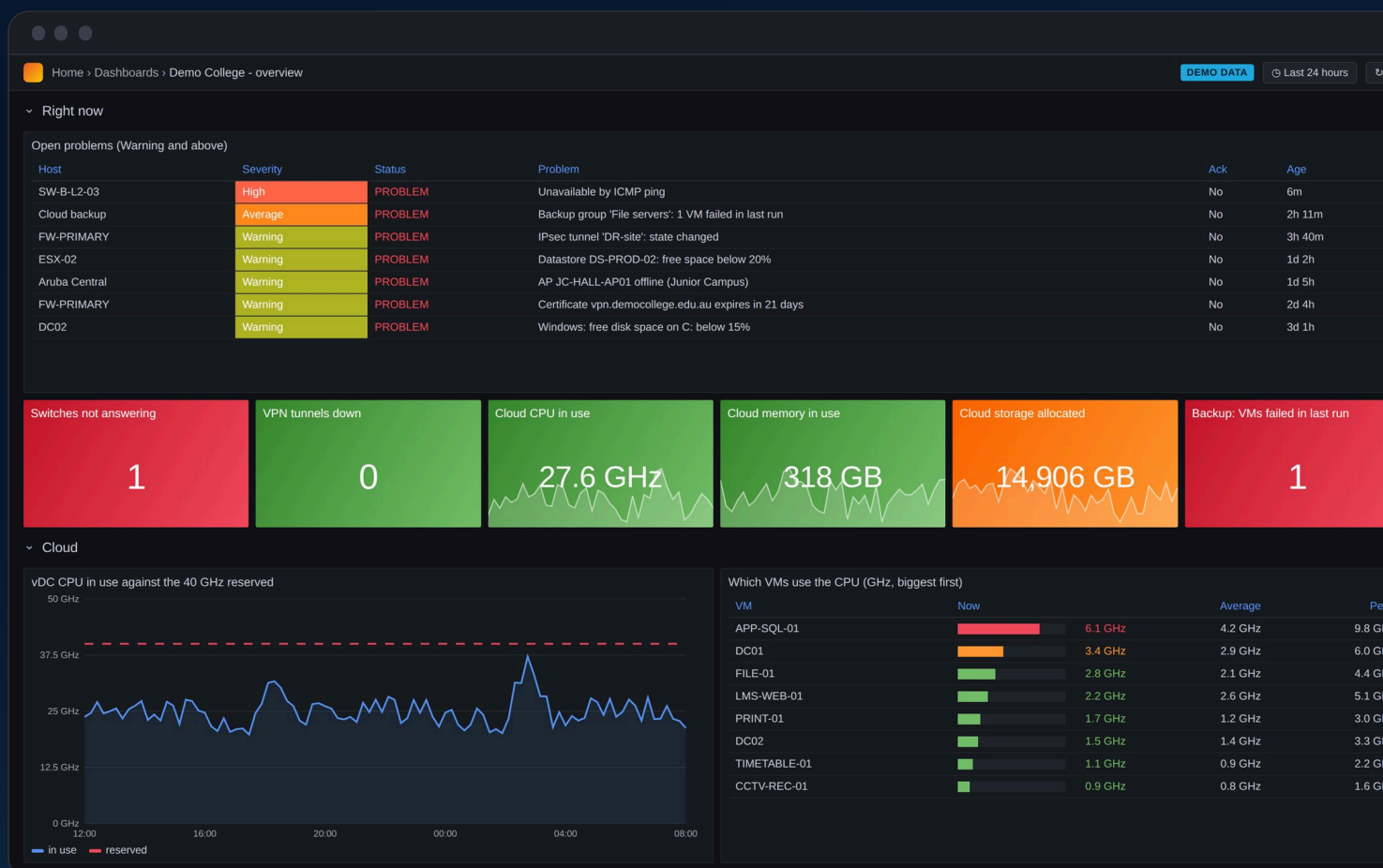


MONITORING FOR AUSTRALIAN BUSINESSES

Know about the problem before your staff do.

One dashboard for every office, site and system: internet, firewalls, Wi-Fi, servers, storage, backups, CCTV, door access and UPS. Watched around the clock, with plain-English alerts to the people who can fix it.



Proactive

Problems found by us, not reported by your staff.

Problems first

What needs attention now, then every area in detail.

Secure by design

Read-only access, hosted in Australia.

SOUND FAMILIAR?

IT teams are stretched. Problems shouldn't be found by users.

A business runs on more systems than ever, spread across offices and sites and supplied by different vendors, each with its own console or none at all. Nobody has time to check them all, every day.

"The Wi-Fi is down"

In the middle of a client presentation, and the first you hear of it is a queue at the IT desk.

The backup that quietly failed

Three weeks ago, discovered on the day a file server needs restoring.

The UPS that ran flat

In a power cut at the warehouse, taking the switch and access points with it.

The camera that was offline

On exactly the night the footage was needed.

WITH ALTITUDO

Every system watched, every minute, from one place.

24/7

monitoring, with history kept for trend and capacity planning

12

kinds of system in one dashboard, across every site

6 weeks

from first workshop to fully monitored and tuned

100%

read-only: we watch your systems, we never change them



Found before it bites

A UPS on battery, a full datastore or a failed backup is an alert, not a surprise.



Alerts that make sense

Plain English, naming the site and device, and an all-clear when it's fixed.



The right person, first time

Alerts go to the people who can act on them, by site and device.



Organised by area

Network, Wi-Fi, servers, cloud and backups each have their own section.



History you can plan with

Trends show when storage will fill, when Wi-Fi peaks and what uses the cloud you pay for.



Nothing to maintain

We run, patch and back up the platform. You get the answers.

WHAT WE MONITOR

From the internet link to the last UPS.

Whatever brands you run, from Palo Alto, Fortinet, Aruba, Meraki and Ubiquiti to HPE, Dell, VMware and Veeam, we bring them into one picture using each vendor's own read-only interfaces.

 Internet links Up or down, latency, packet loss and bandwidth for every link and failover.	 Firewalls Health, HA state, VPN tunnels, licences and certificate expiry.	 Switches Every switch up, with uplinks, errors and PoE where it matters.
 Wi-Fi Access points, clients, and why a device couldn't connect.	 Servers and VMware Hosts, VMs, CPU, memory, datastores, snapshots and hardware.	 SAN and NAS Disk and controller health, capacity, and when it will be full.
 Backups Every job's last result, so a failed backup is never a surprise.	 Cloud and Microsoft 365 Hosted servers, cloud backup and the services staff rely on.	 CCTV Recorders, storage and every camera online. Never the footage.
 PA and building systems Controllers, amplifiers and the network they run on.	 Door and gate access Controllers and servers up, with tamper and offline alerts.	 UPS On battery, runtime remaining, battery health and load.

THE OVERVIEW BOARD

- ✓ **Right now:** every open problem, worst first, with how long it has been open.
- ✓ **The numbers that matter** in green, amber or red: switches not answering, VPN tunnels down, cloud CPU, memory and storage against what you pay for, and failed backups.
- ✓ **Then a section for each area:** cloud, backups, network and on-site VMware, plus a board of its own for Wi-Fi.

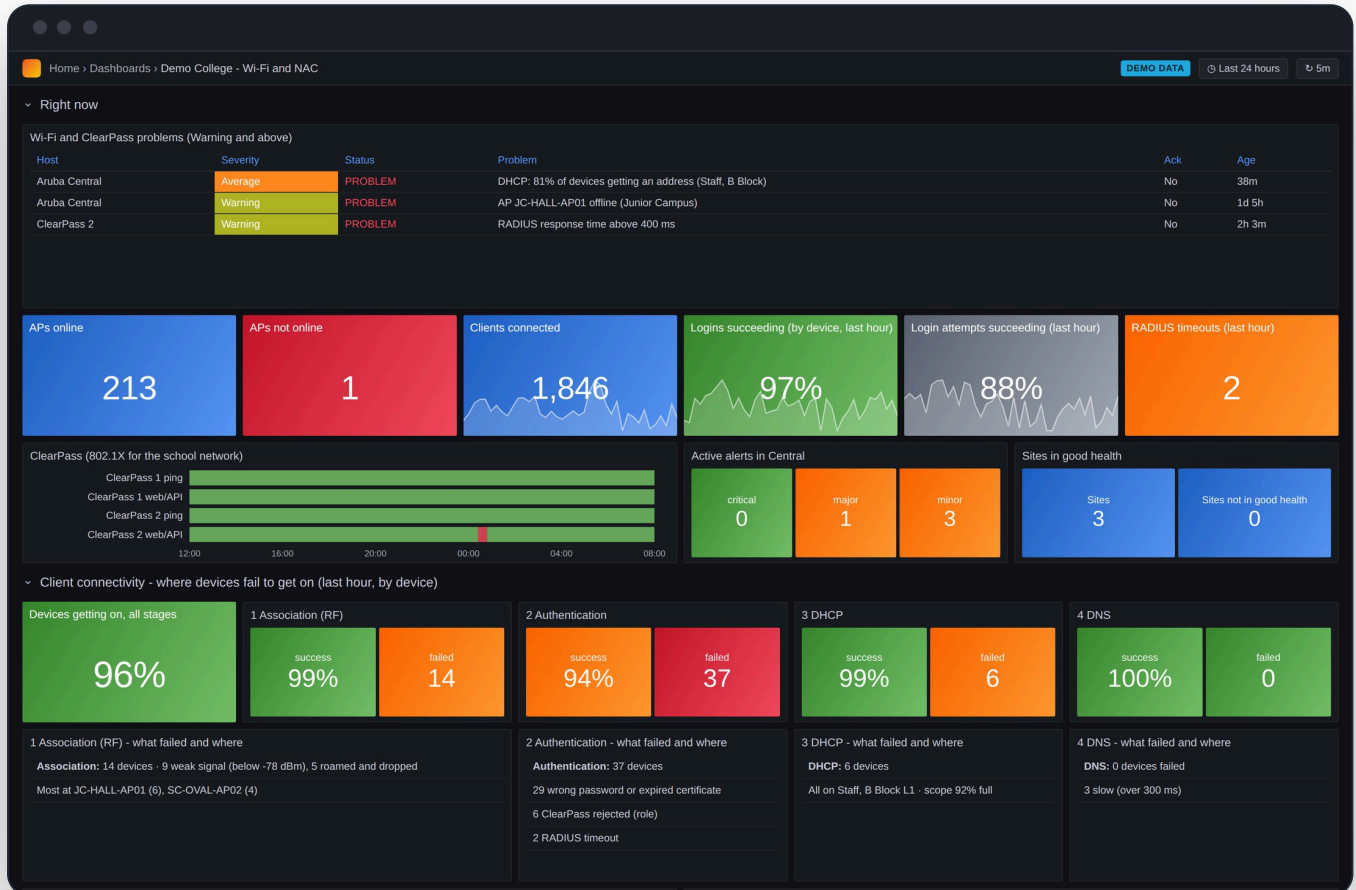
THRESHOLDS TUNED TO YOUR BUSINESS

We learn your normal, from Monday-morning Wi-Fi peaks to overnight backup windows, so alerts mean something. Planned work goes in a maintenance window, and one failure produces one alert, not fifty.

WI-FI THAT EXPLAINS ITSELF

“Why can’t my laptop connect?” Answered in seconds.

Connecting to Wi-Fi takes four steps: the radio, the login, an IP address and a name lookup. We measure every one, for every device, so you can see which step is failing, and for whom.



Wi-Fi and network access board (demonstration data)



Stage by stage

Success rates for association, authentication, DHCP and DNS. A dip in one stage points straight at the cause: RF, RADIUS, a full DHCP scope or DNS.



What failed, and where

Under each stage, what went wrong (wrong passwords, ClearPass rejections, a full DHCP scope, weak signal) and the access points it happened at.



Logins and access points

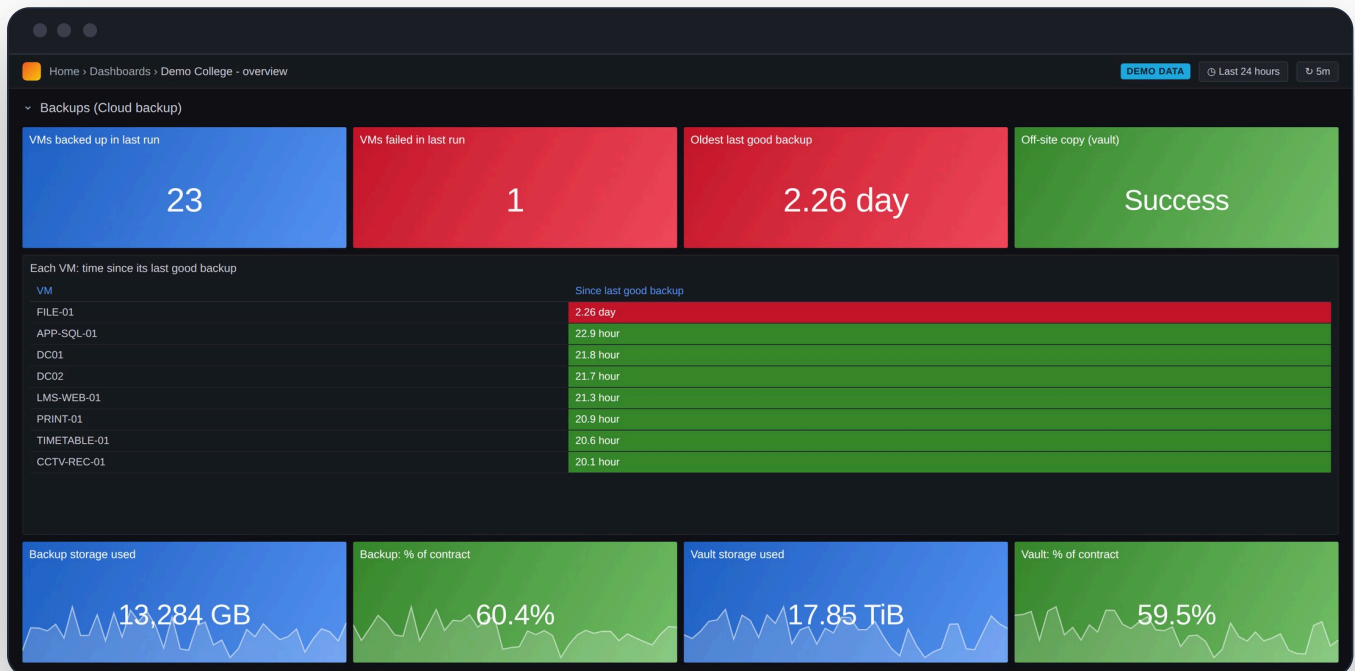
Login success by device and by attempt, RADIUS timeouts, ClearPass health, and access points online or offline, with an alert when it happens.

Shown here with Aruba Central and ClearPass. Other Wi-Fi platforms with an API can be added. Failed logins are counted by device, not by attempt, so one laptop retrying all morning is one problem, not hundreds.

THE CORE OF THE BUSINESS

Servers, storage, backups and power, covered.

The systems nobody looks at until they fail. We watch them every minute and warn you early: a datastore filling up, a backup that failed last night, a switch that has stopped answering.



Backups section of the overview board (demonstration data)

ALERTS PEOPLE ACT ON

The right message, to the right person.

- ✓ **Plain English:** which site, which device, what is wrong and since when.
- ✓ **Only your organisation:** every email names your organisation, and nobody else's alerts reach you.
- ✓ **Severity you set:** High and Disaster by email, the rest on the dashboard.
- ✓ **An all-clear too:** a resolved message when it's fixed, with how long it lasted.
- ✓ **No alert storms:** access points restarting for a firmware upgrade arrive as one summary, not dozens.

Altitude alerts (Demo College): 1 new - SW-B-L2-03: Unavailable by ICMP ping
alerts@altitude.com.au · 10:42 am

Something on the network needs attention.
Customer: **Demo College**

New

HIGH **SW-B-L2-03: Unavailable by ICMP ping**
Zabbix · since 10:36:12 2026,10.09 Sydney time

[Open in Zabbix](#)

Altitude alerts (Demo College): 1 resolved - SW-B-L2-03: Unavailable by ICMP ping
11:01 am

This has cleared.

Resolved

RESOLVED **SW-B-L2-03: Unavailable by ICMP ping**
Zabbix · resolved at 11:00:48 Sydney time, after 24m 36s

SECURE BY DESIGN

Monitoring that never becomes a risk.

Built around Confidentiality, Integrity and Availability, and aligned with the Privacy Act, the Notifiable Data Breaches scheme and the ACSC Essential Eight.

**Confidentiality**

Hosted in Australia (AWS Sydney) and encrypted end to end. No video, audio, customer or staff records are collected, only technical health. Each organisation sees only its own data.

**Integrity**

Strictly read-only: dedicated read-only accounts and API keys, so the platform cannot change a firewall rule, a switch or a camera. Our own configuration is version-controlled.

**Availability**

Outbound-only connection, with no inbound ports opened at your sites. Collectors buffer through internet outages, and the platform monitors itself.

HOW IT WORKS: LIVE IN ABOUT SIX WEEKS

1

Discover

A workshop with your IT team to list sites, systems and what matters most.

2

Connect

A small collector VM at each site. We onboard every system with read-only access.

3

Tune and hand over

Two weeks learning your normal, then dashboards, alerts, reports and training.

FULLY MANAGED

We host, patch and back up the platform, tune the alerts, and add new devices as you add them. Your team just gets the answers.

NEXT STEP

See it on your own network

Book a 30-minute demo, or a discovery session where we map your sites and systems and put together a proposal for your business.



sales@altitudo.com.au

02 8660 1544

altitudo.com.au/service/network-monitoring