

Guide pratique NacTrack

Des réponses opérationnelles, pas à pas, capturées sur une installation réelle.

15 entries · generated 2026-08-02

Sommaire

1. LOCALISER · TERMINAUX

Comment trouver sur quel switch et quel port se trouve une adresse MAC

2. LOCALISER · TERMINAUX

Comment trouver où vit une adresse IP sur le réseau

3. LOCALISER · TERMINAUX

Comment chercher avec une adresse MAC partielle pour trouver tous les terminaux d'un même fabricant

4. LOCALISER · TERMINAUX

Comment savoir si une adresse IP appartient à un poste utilisateur ou à un équipement réseau

5. LOCALISER · VLAN ET COUCHE 2

Comment trouver tous les ports qui portent un VLAN

6. LOCALISER · VLAN ET COUCHE 2

Comment voir quels VLAN un trunk autorise

7. COMPRENDRE · POSTURE DE SÉCURITÉ

Comment voir quels ports sont configurés pour le 802.1X

8. COMPRENDRE · POSTURE DE SÉCURITÉ

Comment vérifier si un équipement autorise encore Telnet

9. COMPRENDRE · POSTURE DE SÉCURITÉ

Comment repérer les équipements utilisant des communautés SNMP par défaut ou en version 1 et 2c

10. COMPRENDRE · POSTURE DE SÉCURITÉ

Comment lire la posture d'accès de gestion d'un équipement

11. COMPRENDRE · SPANNING TREE

Comment trouver quel switch est pont racine pour chaque VLAN

12. COMPRENDRE · SPANNING TREE

Comment trouver quels ports le spanning tree bloque

13. COMPRENDRE · SPANNING TREE

Comment vérifier si BPDU Guard est activé sur les ports d'accès

14. COMPRENDRE · VLAN ET COUCHE 2

Comment savoir si un VLAN a encore des ports sur un switch

15. DIAGNOSTIQUER · CHANGEMENT ET PANNE

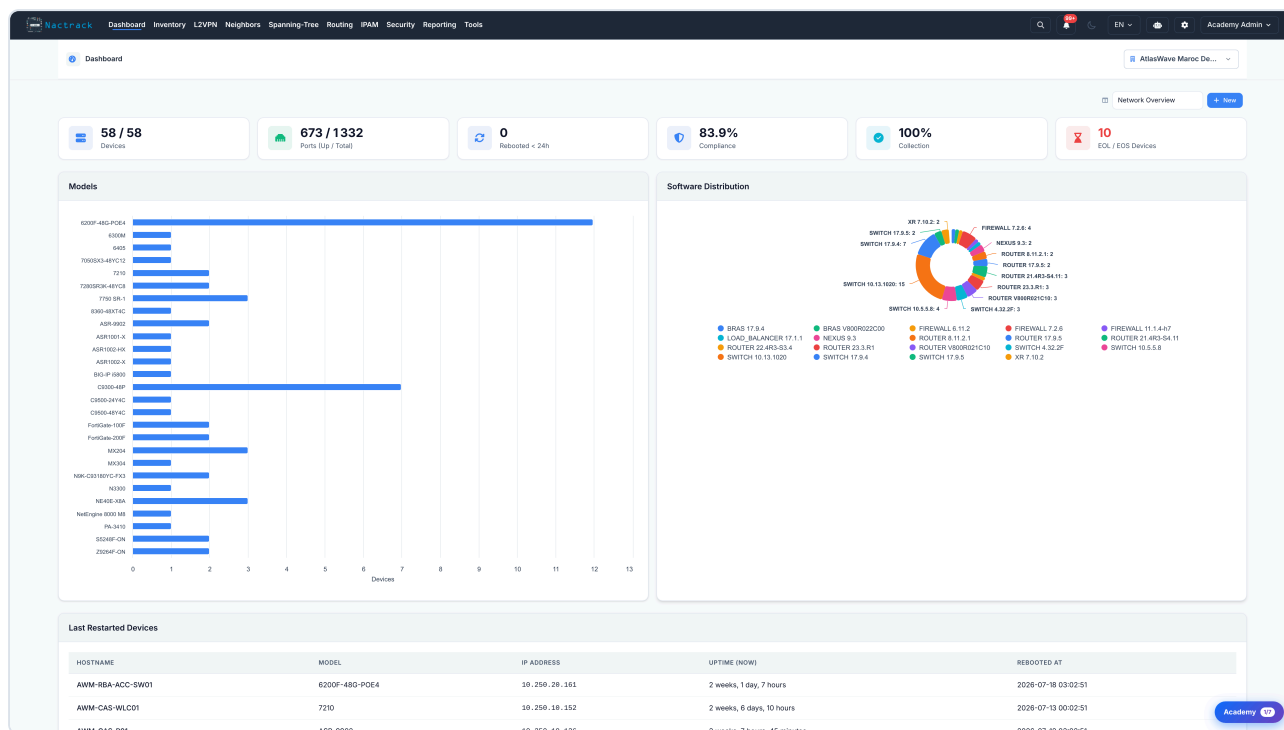
Comment savoir ce qui a changé sur le réseau entre deux collectes

Comment trouver sur quel switch et quel port se trouve une adresse MAC

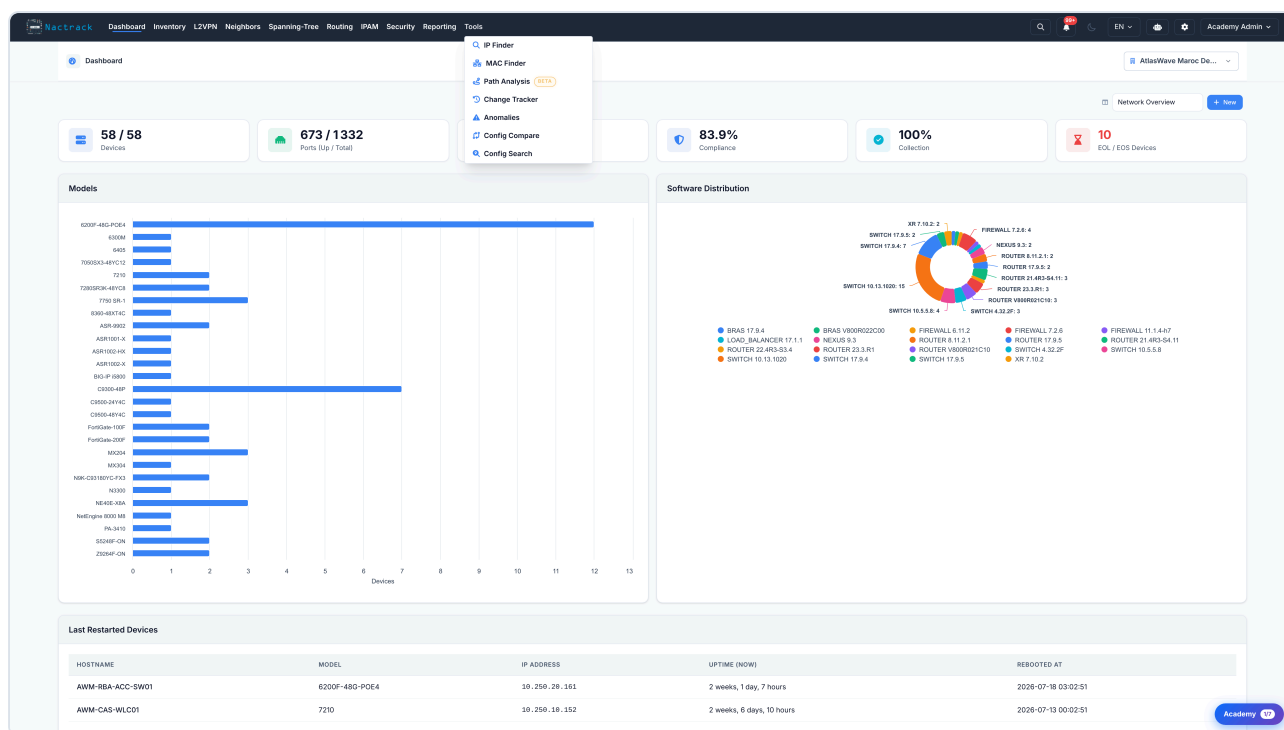
Un utilisateur signale un incident et vous n'avez qu'une adresse MAC. MAC Finder interroge en une fois toutes les tables MAC collectées sur le parc et vous indique l'équipement, l'interface et le VLAN d'apprentissage. Il lit la dernière collecte, pas le switch en direct : la réponse est donc aussi récente que votre dernier cycle de collecte.

Nécessite: module: core, permission: use_troubleshooting

- 1 Nous partons du tableau de bord NacTrack, la dernière collecte étant déjà chargée. Localiser un terminal est une tâche de dépannage : tout ce dont nous avons besoin se trouve donc dans un seul menu.



- 2 Ouvrez le menu Tools dans la barre de navigation. C'est ici que NacTrack regroupe les outils qui répondent à une question sur un élément précis, plutôt que d'afficher un inventaire complet.



- 3 Choisissez MAC Finder. La page s'ouvre vide, avec un seul champ de recherche : elle ne contient aucune liste propre et ne cherche que ce que vous lui demandez. Tout ce qu'elle renvoie provient des tables MAC collectées sur vos switches.

The screenshot shows the NacTrack MAC Finder tool interface. It features a search bar labeled 'MAC Address / IP Address' with a dropdown menu showing 'aa:bb:cc:dd:ee:ff / aa:bb:cc:dd:ee:ff / 10.0.0.1'. Below the search bar, there are 'Find' and 'Reset' buttons. A note indicates 'Wildcards supported, e.g. aa:bb*, 10.0.0.*, aa:bb:cc*'. The interface is clean and ready for input.

- 4 Saisissez l'adresse MAC recherchée. Les formats à deux-points, à points et à tirets sont acceptés : vous pouvez la coller telle quelle depuis votre ticket, sans la reformater.

Le champ de recherche de cette page n'est pas celui de la barre de navigation, qui recherche des adresses IP.

The screenshot shows the NacTrack MAC Finder tool interface with the MAC address '3c:97:0e:68:41:41' entered in the search bar. The 'Find' and 'Reset' buttons are still visible. The interface remains clean and ready for further action.

- 5 Cliquez sur Find. Tous les switches ayant appris cette adresse répondent en une fois. Lisez la ligne de gauche à droite : l'adresse, l'IP associée, le VLAN, l'interface, l'équipement qui porte cette interface, la VRF, et l'ancienneté de l'apprentissage.

The screenshot shows the Nactrack MAC Finder interface. The search criteria are MAC Address / IP Address: 3c:97:0e:68:41:41. The search results show 14 entries found. The table below represents the data shown in the screenshot.

MAC ADDRESS	IP ADDRESS	VLAN	INTERFACE	DEVICE	TYPE	VRF	AGE	COLLECTED
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-CAS-DC-SP01	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-CAS-DC-SP03	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	ethernet1/10	AWM-CAS-DC-LF04	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-CAS-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-RBA-CORE-SW01	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-RBA-AGG-SW01	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-MRT-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-TNG-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-FES-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	100	Gi1/0/14	AWM-AGA-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	-	Vlan100	AWM-CAS-DC-LF01	Asp	VRF-DC-SHARED	229	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	-	Vlan100	AWM-CAS-DC-LF02	Asp	VRF-DC-SHARED	91	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	-	Vlan100	AWM-CAS-DC-LF03	Asp	VRF-DC-SHARED	197	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.100.0.103	-	Vlan100	AWM-CAS-DC-LF04	Asp	VRF-DC-SHARED	50	2026-07-31T14:02:51

BON À SAVOIR

Une MAC renvoie normalement plusieurs lignes. Tous les switches du chemin l'ont apprise : les liens montants apparaissent donc à côté du port d'accès. Le port d'accès est celui dont l'interface n'est pas un trunk vers un autre switch.

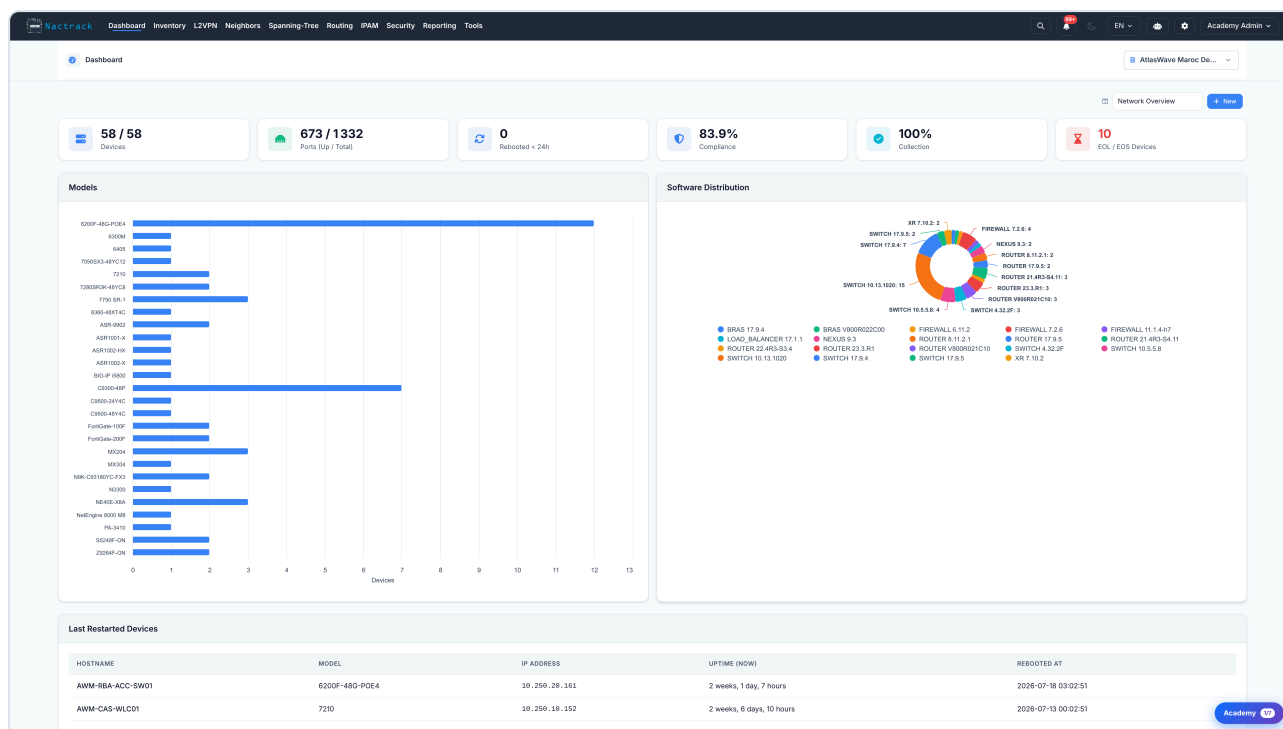
La colonne IP n'est renseignée que si la même adresse a été vue dans une table ARP. Une IP vide signifie que le terminal est purement niveau 2, ou qu'aucun routeur du chemin ne l'a résolue en ARP.

Comment trouver où vit une adresse IP sur le réseau

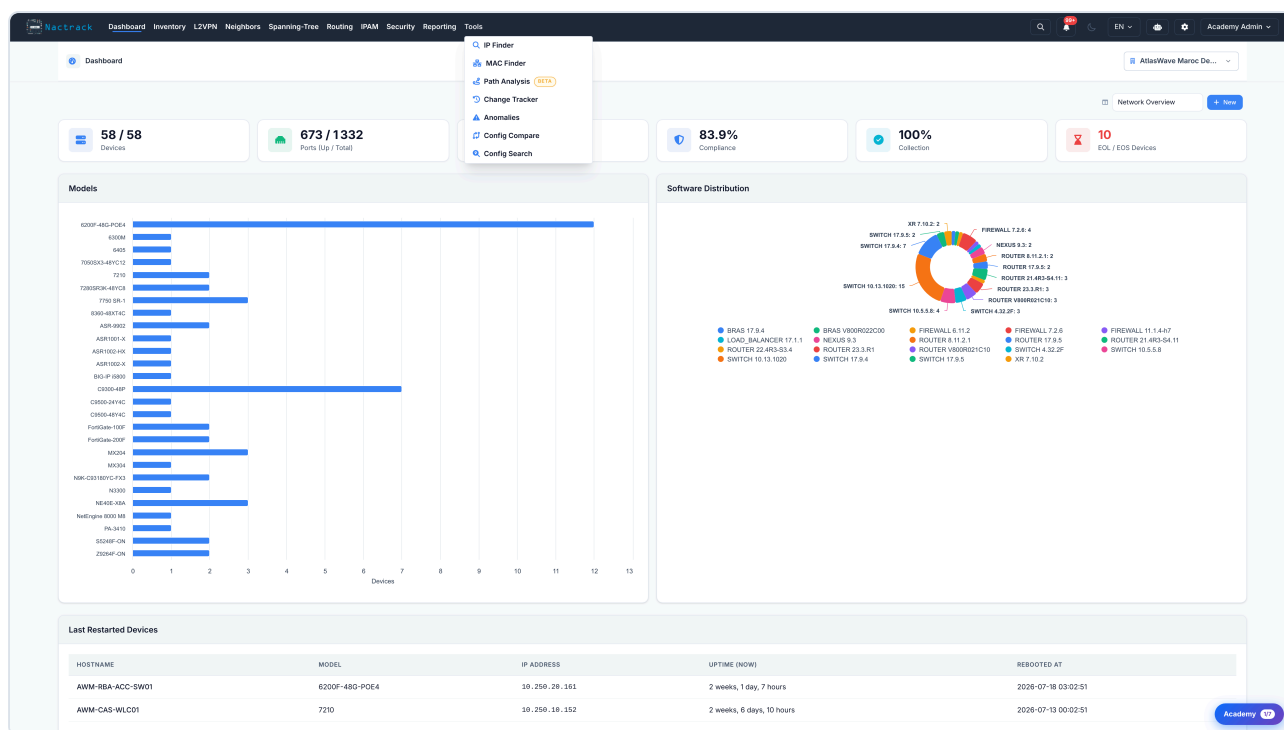
Vous avez une adresse IP et devez savoir quel équipement la porte et derrière quelle interface. IP Finder interroge toutes les sources collectées par NacTrack - tables ARP, inventaire et tables de voisinage - et regroupe la réponse par source, ce qui permet de distinguer d'un coup d'oeil un terminal d'une adresse de management.

Nécessite: module: core, permission: use_troubleshooting

- 1 Nous repartons du tableau de bord, la dernière collecte étant chargée. Retrouver une adresse est une recherche ponctuelle et non un rapport : nous passons donc par le même menu de dépannage.



- 2 Ouvrez le menu Tools. IP Finder se trouve en haut de la liste, juste au-dessus de MAC Finder : les deux sont complémentaires, l'un partant d'une adresse, l'autre d'un identifiant matériel.



- 3 Choisissez IP Finder. Comme MAC Finder, la page s'ouvre avec un seul champ et aucune liste propre, et elle accepte aussi bien une adresse d'hôte qu'un sous-réseau entier en notation CIDR.

The screenshot shows the IP Finder tool interface with the following elements:

- Navigation:** Tools > IP Finder
- Search Field:** A dropdown menu showing "IP/Subnet" with the value "192.0.2.7 or 198.51.100.0/24".
- Buttons:** Find, Reset

- 4 Saisissez l'adresse recherchée.

The screenshot shows the IP Finder tool interface with the following elements:

- Navigation:** Tools > IP Finder
- Search Field:** A dropdown menu showing "IP/Subnet" with the value "10.100.0.103".
- Buttons:** Find, Reset

- 5 Cliquez sur Find. Le bloc est titré par la source qui a répondu, ici la table ARP, et chaque ligne nomme l'équipement qui détient l'entrée, l'interface, la VRF et l'adresse MAC située derrière cette IP.

The screenshot shows the Nactrack IP Finder interface. The search bar contains the IP address 10.100.0.103. Below the search bar, the results are displayed under the heading "ARP Table (4)". The table lists four entries, each representing a different host (AWM-CAS-DC-LF01 to AWM-CAS-DC-LF04) that has responded to the IP address. Each entry includes the host name, IP address, MAC address, interface, VRF, and details.

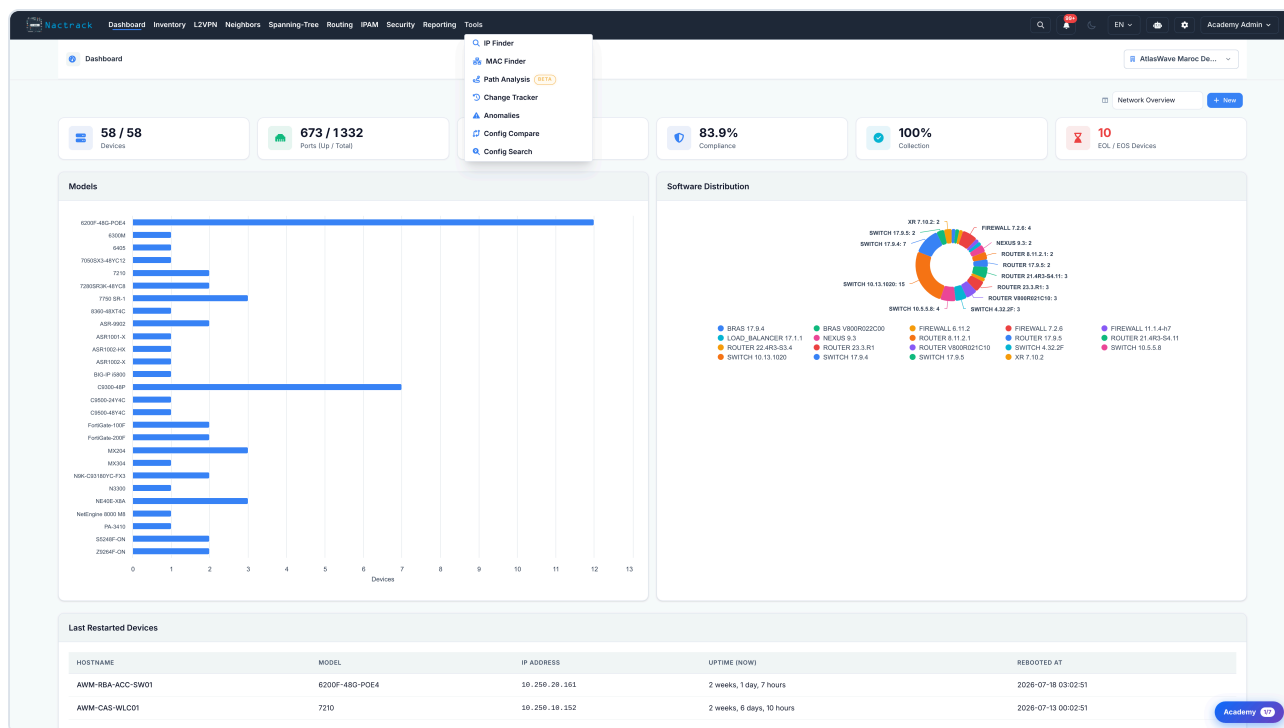
HOSTNAME	IP ADDRESS	MAC ADDRESS	INTERFACE	VRF	DETAILS
AWM-CAS-DC-LF01	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 229
AWM-CAS-DC-LF02	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 81
AWM-CAS-DC-LF03	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 187
AWM-CAS-DC-LF04	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 50

BON À SAVOIR

Plusieurs équipements répondent normalement pour la même IP de terminal. Chacun est un routeur ou une interface virtuelle qui possède l'adresse dans sa propre table ARP : ce ne sont pas des doublons.

La réponse n'est fraîche que jusqu'à la dernière collecte. Une entrée ARP expirée depuis sur l'équipement reste affichée jusqu'au prochain cycle de collecte.

2 Ouvrez de nouveau le menu Tools.



3 Choisissez MAC Finder. Remarquez l'indication sous le champ : les jokers sont pris en charge. Cette simple ligne transforme un outil de recherche en outil d'inventaire.

The screenshot shows the Nactrack MAC Finder tool. The interface includes a search bar for MAC Address / IP Address and a 'Find' button. Below the search bar, there is a note: 'Wildcards supported, e.g. aa:bb*:10.0.0*, aa:bb:cc*'. The search bar contains the text 'aa:bb:cc:dd:ee:ff / 10.0.0.1'.

4 Saisissez le préfixe du fabricant suivi d'une étoile. Trois octets est la longueur habituelle d'un préfixe constructeur, mais toute adresse partielle fonctionne.

The screenshot shows the Nactrack MAC Finder tool with the search bar containing the text '00:1c:b3*'. The 'Find' button is visible below the search bar.

- 5 Cliquez sur Find. Tous les terminaux dont l'adresse commence par ce préfixe remontent, sur tous les switches et tous les sites, chacun avec son port de rattachement. Ce qui était une réponse unique devient une population que vous pouvez compter.

MAC Address / IP Address

00:1c:b3:07:7b:29

Wildcards supported, e.g. aa:bb*:10.0.0.*,aa:bb:cc*

Find Reset

120 results found

CSV Excel

Show 50 entries

Search:

MAC ADDRESS	IP ADDRESS	VLAN	INTERFACE	DEVICE	TYPE	VRF	AGE	COLLECTED
MAC Address	IP Address	VLAN	Interface	Device	Type	VRF	Age	Collected
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-CAS-CORE-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-CAS-AGG-SW02	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-RBA-ACC-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-MRT-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-TNG-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-FES-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-AGA-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-OLD-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-CAS-CORE-SW02	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	ethernet1/10	AWM-CAS-DC-LF01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	ethernet1/1	AWM-CAS-DC-LF02	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	ethernet1/1	AWM-CAS-DC-LF04	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-CAS-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-RBA-ACC-SW02	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-MRT-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-TNG-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-FES-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-AGA-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF01	Arp	VRF-DC-SHARED	27	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF02	Arp	VRF-DC-SHARED	121	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF03	Arp	VRF-DC-SHARED	4	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF04	Arp	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:25:38:53	-	20	Gi1/0/2	AWM-CAS-DC-SP02	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:25:38:53	-	20	Gi1/0/2	AWM-CAS-DC-SP04	Dynamic	-	-	2026-07-31T14:02:51

BON À SAVOIR

Un préfixe constructeur ne prouve pas le type d'équipement. Il indique qui a fabriqué la puce réseau, ce qui sur un hôte virtualisé désigne l'éditeur de l'hyperviseur et non la marque de la machine.

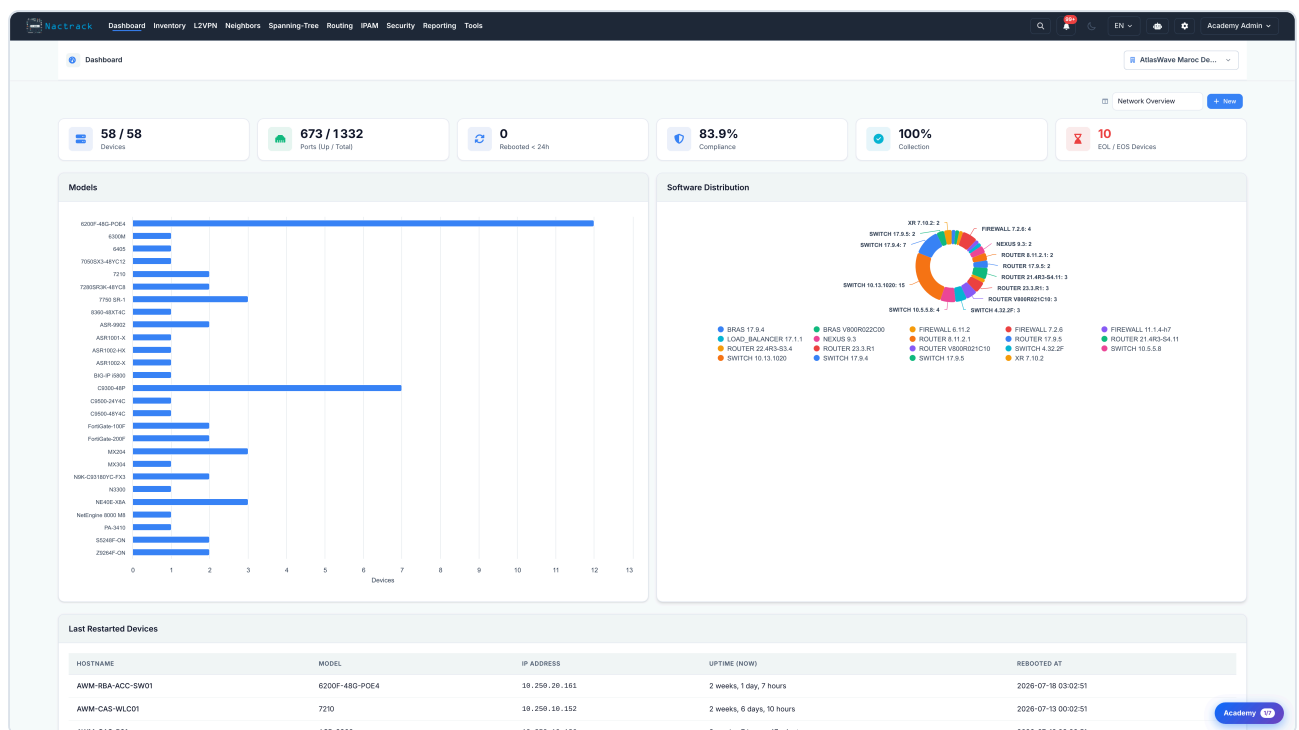
Les résultats sont plafonnés à l'affichage. Affinez le préfixe, ou filtrez par équipement, si la liste dépasse ce que la page montre.

Comment savoir si une adresse IP appartient à un poste utilisateur ou à un équipement réseau

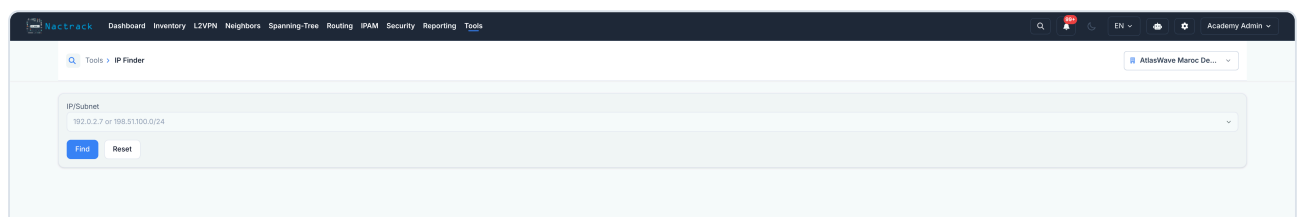
IP Finder titre chaque bloc de résultats par la source qui a répondu, et ce titre répond à une question posée en permanence. Une adresse trouvée dans une table ARP correspond à quelque chose de branché sur le réseau. Une adresse trouvée dans l'inventaire correspond à un équipement géré par NacTrack. Le même champ de recherche vous le dit, sans le savoir à l'avance.

Nécessite: module: core, permission: use_troubleshooting

- 1 Depuis le tableau de bord une fois encore. Cette fois la leçon ne porte pas sur la recherche mais sur la lecture du résultat, car IP Finder répond à une question que vous n'avez pas posée explicitement.

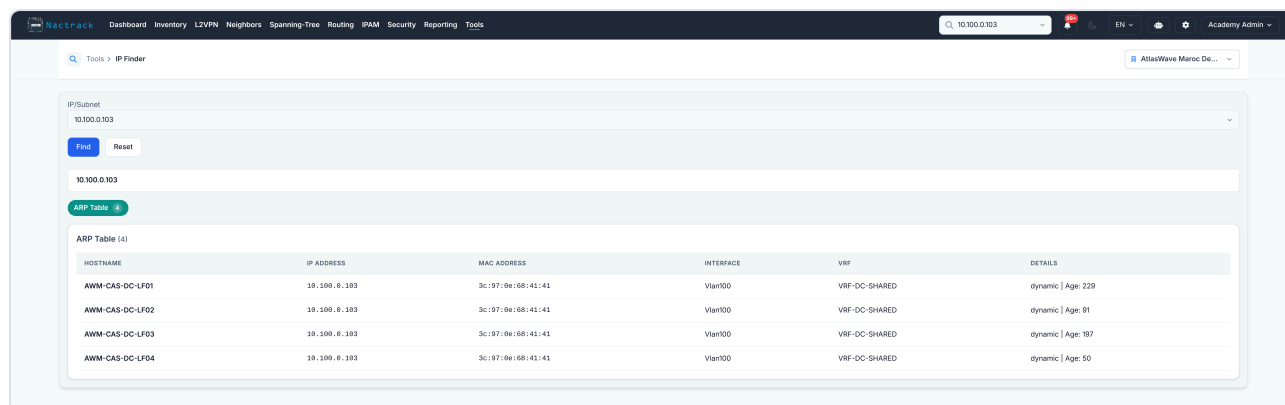


- 2 Ouvrez Tools et choisissez IP Finder.

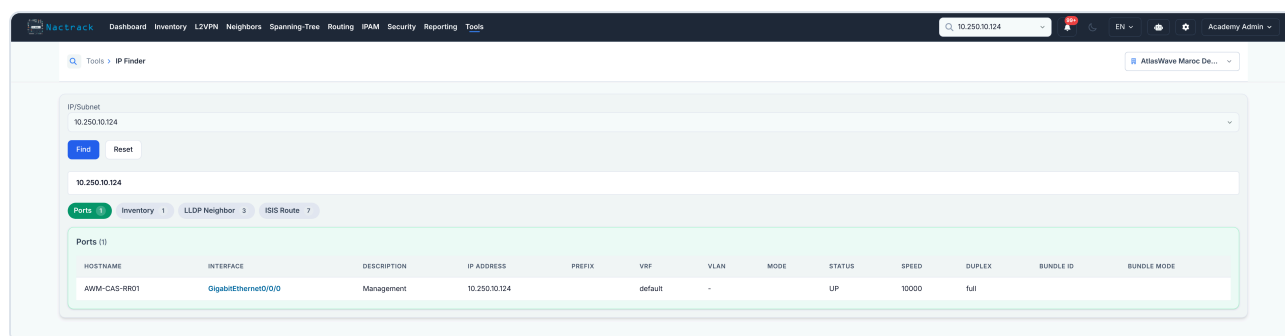


- 3 Commencez par une adresse portée par un poste utilisateur.

- 4 Le bloc est titré ARP Table. NacTrack ne connaît cette adresse que parce que des routeurs l'ont résolue, ce qui signifie qu'il s'agit de quelque chose de branché sur le réseau et non d'un de ses composants.



- 5 Effacez maintenant le champ et cherchez plutôt une adresse de management.
- 6 Le titre est devenu Inventory, et un second bloc est apparu pour le voisin LLDP qui voit cette adresse. Même champ, même syntaxe, et la réponse vous dit à quel type d'objet vous avez affaire.



BON À SAVOIR

Les sections affichées dépendent entièrement de ce qui a été collecté. Un terminal qu'aucun routeur n'a résolu en ARP depuis la dernière collecte n'apparaîtra pas du tout, même s'il est bien connecté.

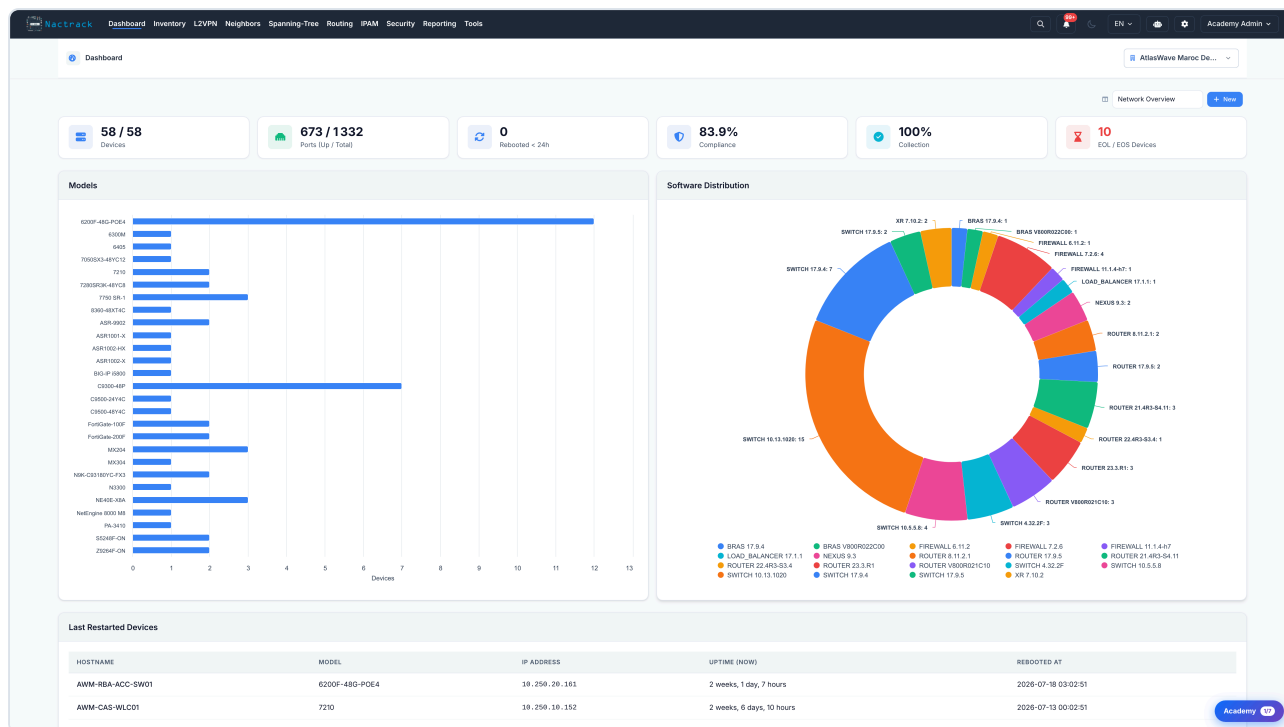
Une adresse peut légitimement apparaître sous plusieurs sources à la fois. C'est une confirmation, pas un conflit.

Comment trouver tous les ports qui portent un VLAN

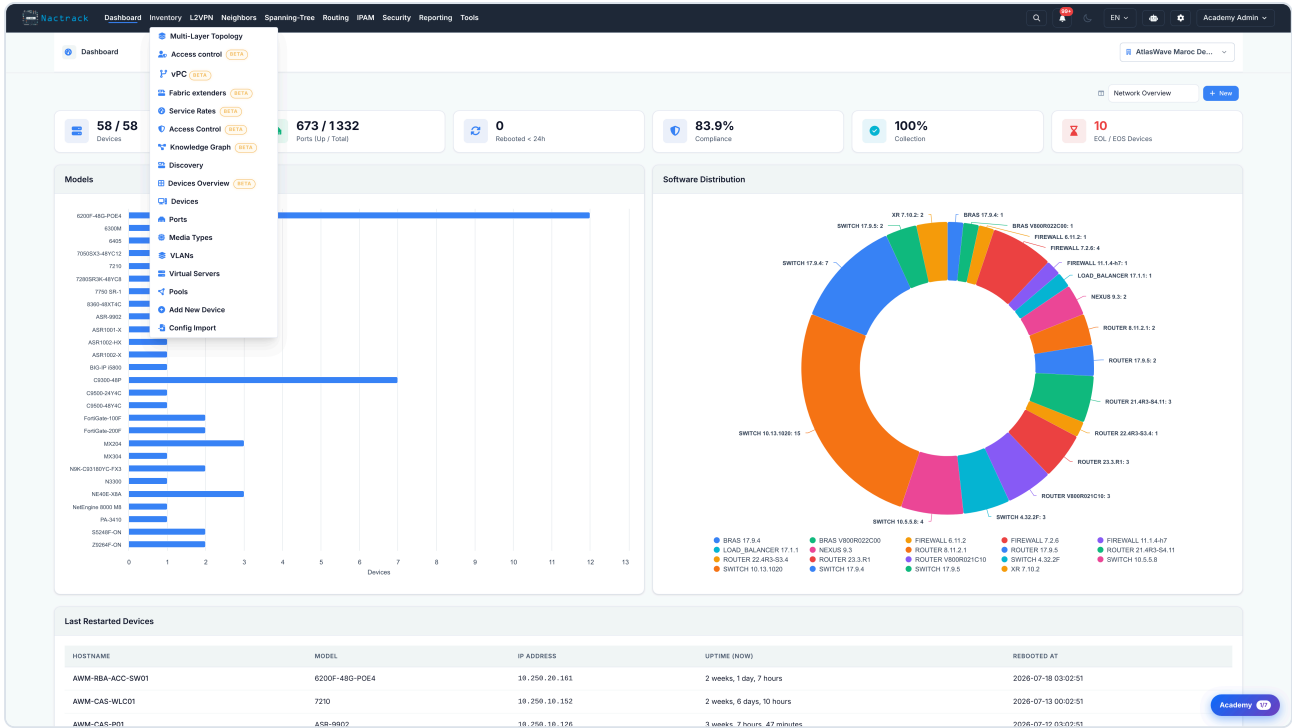
Avant de modifier ou de retirer un VLAN, il faut savoir ce qui l'utilise réellement. L'inventaire VLAN liste chaque VLAN trouvé sur chaque switch, avec les ports qui lui sont affectés : une seule page répond pour tout le parc, au lieu d'un switch à la fois.

Nécessite: module: inventory, permission: view_inventory

- 1 Nous partons du tableau de bord. Une question de VLAN relève de l'inventaire et non du dépannage : nous passons donc cette fois par un autre menu.



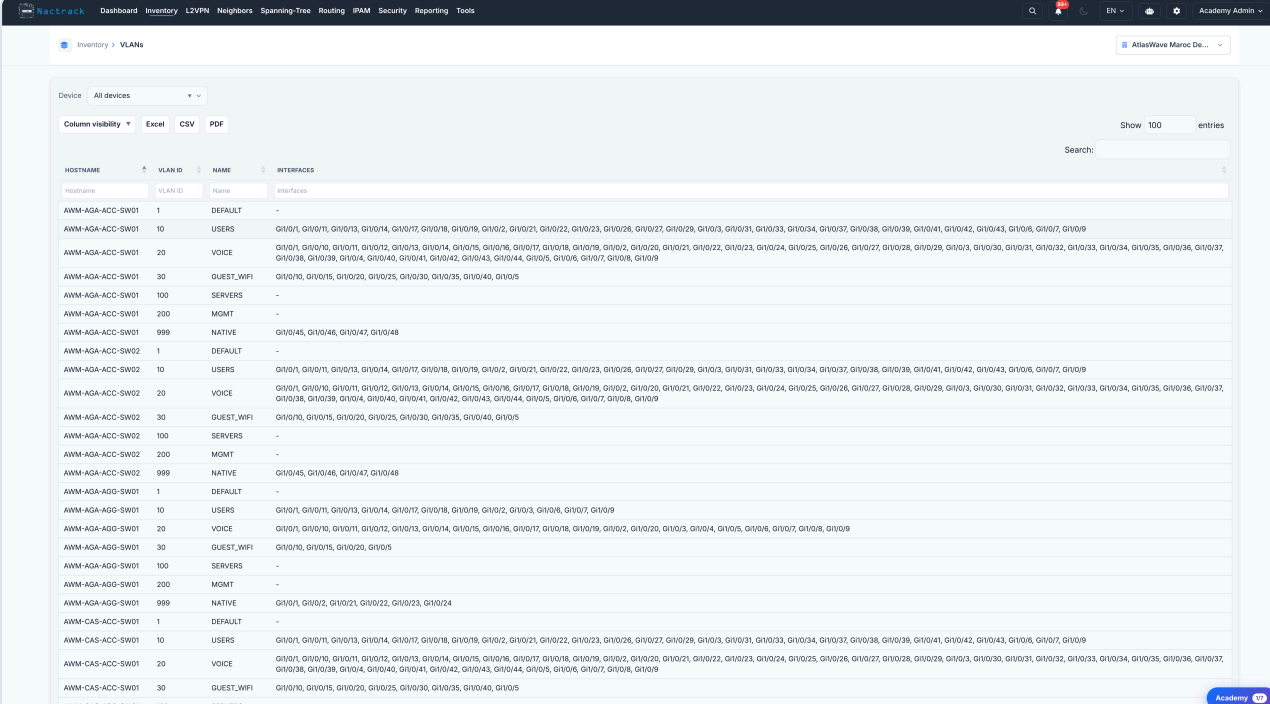
2



3

[illegible]

- 4 Lisez une ligne de gauche à droite : le switch, l'identifiant du VLAN, le nom que le switch lui donne, et les ports qui le portent. Un VLAN défini mais sans port affecté affiche un tiret, ce qui mérite d'être remarqué avant de supposer qu'il est utilisé.



The screenshot shows the Nactrack web interface for the 'Inventory > VLANs' section. The table displays VLAN configurations for various switches, including columns for Hostname, VLAN ID, Name, and Interfaces. The 'Interfaces' column lists the specific ports assigned to each VLAN, such as Gi1/0/1 through Gi1/0/24. Some VLANs are marked as 'DEFAULT' or have specific names like 'USERS', 'VOICE', 'GUEST_WIFI', 'SERVERS', 'MGMT', or 'NATIVE'. The table is paginated, showing 100 entries.

Hostname	VLAN ID	Name	Interfaces
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW01	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/43, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW02	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/43, Gi1/0/44, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-AGA-ACC-SW02	100	SERVERS	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-AGG-SW01	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/3, Gi1/0/6, Gi1/0/7, Gi1/0/9
AWM-AGA-AGG-SW01	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9
AWM-AGA-AGG-SW01	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/5
AWM-AGA-AGG-SW01	100	SERVERS	-
AWM-AGA-AGG-SW01	200	MGMT	-
AWM-AGA-AGG-SW01	999	NATIVE	Gi1/0/1, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-CAS-ACC-SW01	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-CAS-ACC-SW01	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/44, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-CAS-ACC-SW01	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-CAS-ACC-SW01	100	SERVERS	-

BON À SAVOIR

La colonne Interfaces est construite uniquement à partir des affectations de VLAN d'accès, de voix et natif. Elle ne lit PAS la liste des VLAN autorisés sur les trunks : un VLAN transporté sur un lien montant n'y apparaît donc pas. Pour cela, consultez la colonne Allowed VLANs de la page Ports.

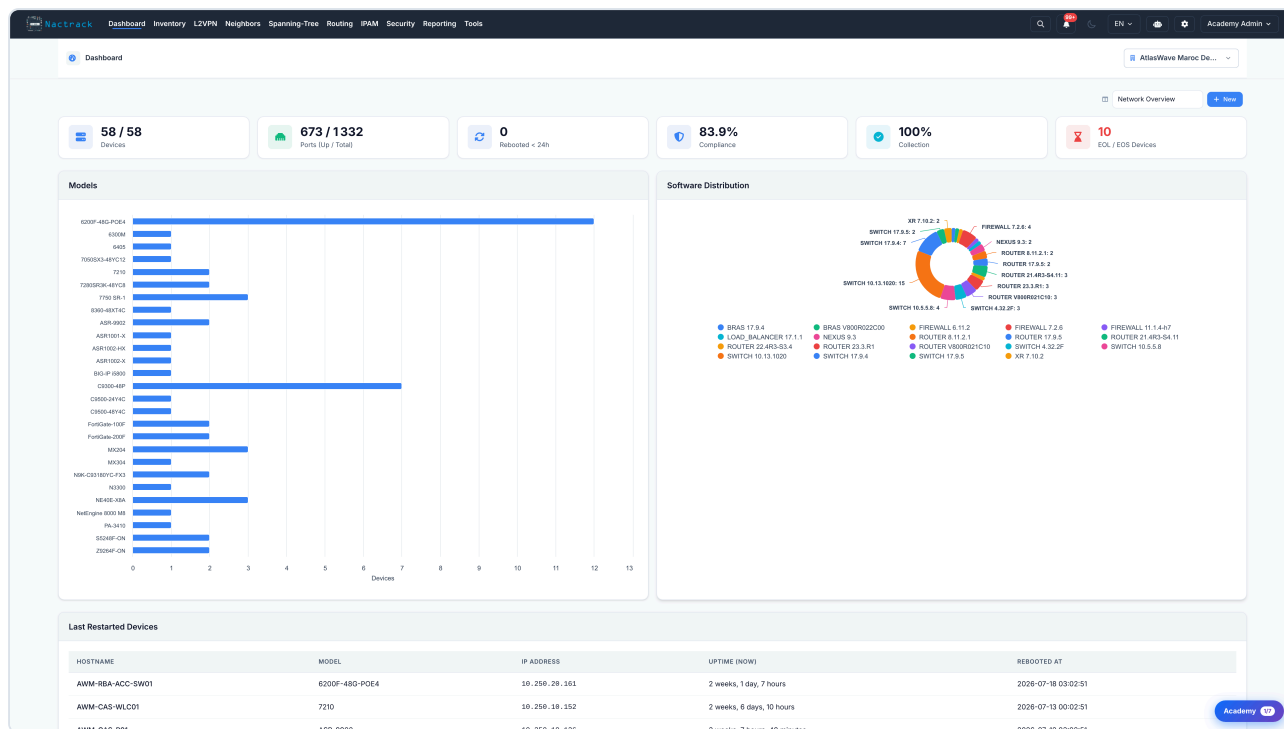
Un même identifiant de VLAN sur deux switches ne correspond pas forcément au même domaine de niveau 2. Ce n'est le même domaine que si un chemin le transporte entre les deux.

Comment voir quels VLAN un trunk autorise

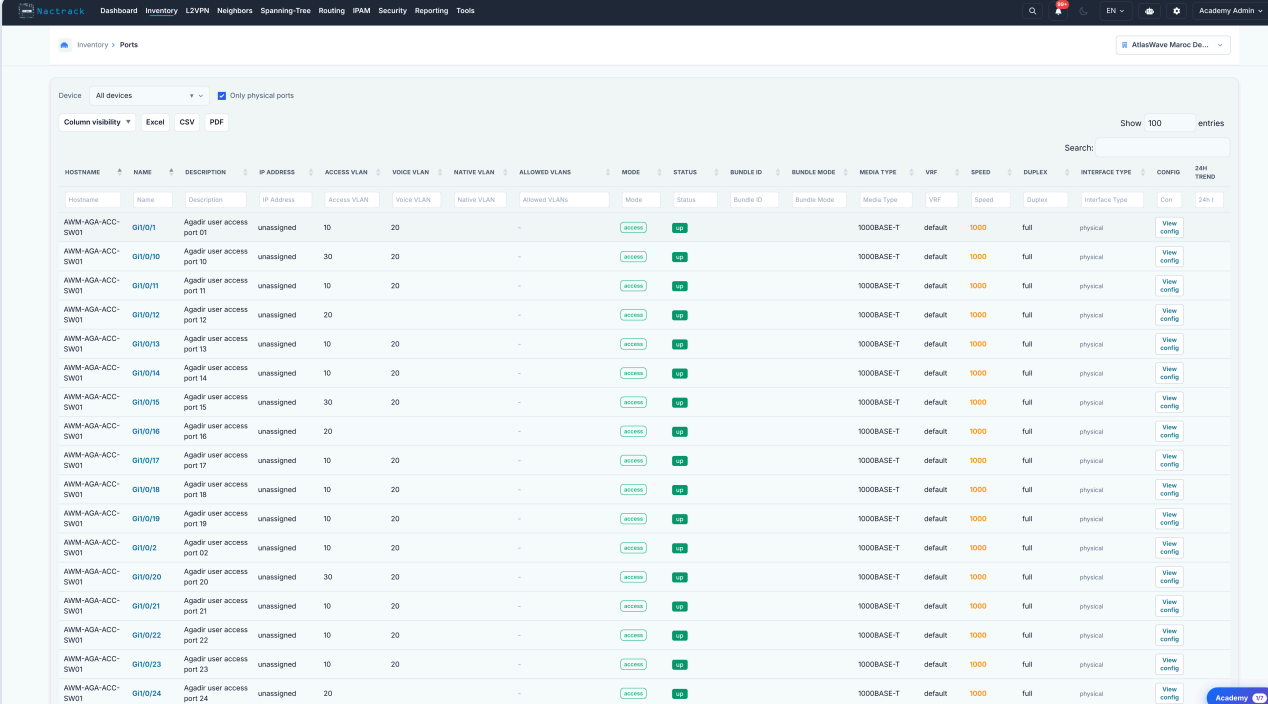
Un VLAN n'atteint un switch distant que si chaque trunk du chemin l'autorise : lorsqu'un VLAN manque sur un site, la liste des VLAN autorisés est donc la première chose à vérifier. L'inventaire des ports affiche les VLAN autorisés et le VLAN natif de chaque trunk du parc, côte à côte.

Nécessite: module: inventory, permission: view_inventory

- 1 De nouveau depuis le tableau de bord. La configuration des trunks fait partie de l'état des interfaces collecté : elle se trouve donc dans Inventory avec le reste des données de port.



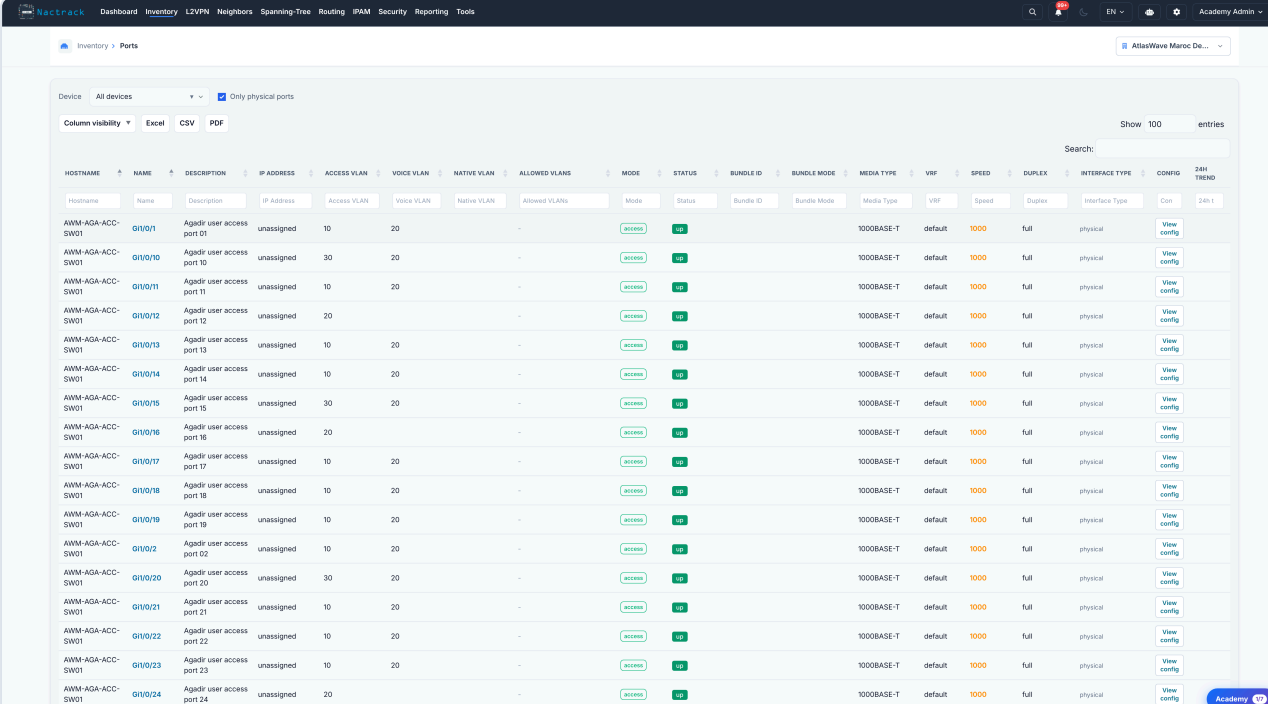
- 2 Ouvrez Inventory et choisissez Ports. Chaque interface physique et logique collectée par NacTrack figure ici, une ligne par interface, d'où la largeur du tableau : il porte le VLAN, le débit, le duplex, le média et la VRF de chacune.



The screenshot shows the NacTrack web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'L2VPN', 'Neighbors', 'Spanning-Tree', 'Routing', 'IPAM', 'Security', 'Reporting', and 'Tools'. The 'Inventory' tab is active, and the 'Ports' sub-tab is selected. The page title is 'Inventory > Ports'. On the right, there's a search bar and a 'Show 100 entries' dropdown. Below the title, there's a filter section with 'Device: All devices' and a checkbox for 'Only physical ports' which is checked. There are also buttons for 'Column visibility', 'Excel', 'CSV', and 'PDF'. The main table has columns: Hostname, Name, Description, IP Address, Access VLAN, Voice VLAN, Native VLAN, Allowed VLANs, Mode, Status, Bundle ID, Bundle Mode, Media Type, VRF, Speed, Duplex, Interface Type, Config, and 24h Trend. The table lists 24 ports for device 'AWM-AGA-ACC-SW01'. Each row shows details for a specific port (e.g., G1/0/1, G1/0/10, etc.), including its description, IP address, and various VLAN assignments. The 'Status' column shows 'UP' for all ports. The 'Speed' is consistently '1000' and 'Duplex' is 'full'. The 'Interface Type' is 'physical'. A 'View config' link is available for each port. At the bottom right, there's an 'Academy' badge.

HOSTNAME	NAME	DESCRIPTION	IP ADDRESS	ACCESS VLAN	VOICE VLAN	NATIVE VLAN	ALLOWED VLANS	MODE	STATUS	BUNDLE ID	BUNDLE MODE	MEDIA TYPE	VRF	SPEED	DUPLEX	INTERFACE TYPE	CONFIG	24h TREND
AWM-AGA-ACC-SW01	G1/0/1	Agadr user access port 01	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/10	Agadr user access port 10	unassigned	30	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/11	Agadr user access port 11	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/12	Agadr user access port 12	unassigned	20	-	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/13	Agadr user access port 13	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/14	Agadr user access port 14	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/15	Agadr user access port 15	unassigned	30	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/16	Agadr user access port 16	unassigned	20	-	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/17	Agadr user access port 17	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/18	Agadr user access port 18	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/19	Agadr user access port 19	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/2	Agadr user access port 02	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/20	Agadr user access port 20	unassigned	30	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/21	Agadr user access port 21	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/22	Agadr user access port 22	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/23	Agadr user access port 23	unassigned	10	20	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/24	Agadr user access port 24	unassigned	20	-	-	-	301000	UP	-	-	1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-	Agadr user access																View	

- 3 Quatre colonnes répondent à la question des VLAN. Access VLAN et Voice VLAN concernent les ports d'accès. Native VLAN et Allowed VLANs concernent les trunks : la liste des autorisés est exactement ce que le trunk transportera, et tout ce qui en est absent est silencieusement écarté à ce saut.



This screenshot is identical to the one above, showing the NacTrack 'Inventory > Ports' page. It displays a table with 24 rows of port information for device 'AWM-AGA-ACC-SW01'. The columns include Hostname, Name, Description, IP Address, Access VLAN, Voice VLAN, Native VLAN, Allowed VLANs, Mode, Status, Bundle ID, Bundle Mode, Media Type, VRF, Speed, Duplex, Interface Type, Config, and 24h Trend. All ports are shown as 'UP' and have a speed of '1000' and duplex of 'full'. The 'Access VLAN' and 'Voice VLAN' columns are populated for each port, while 'Native VLAN' and 'Allowed VLANs' are mostly empty or show a dash. The 'View config' link is present for each port. An 'Academy' badge is visible in the bottom right corner.

BON À SAVOIR

Un VLAN présent dans la liste des autorisés n'est pas forcément défini sur le switch. Cette liste est du texte de configuration : elle peut nommer un VLAN jamais créé, et le trunk ne transportera rien pour lui.

Rien ici ne compte les VLAN d'un trunk ni ne classe les trunks selon leur nombre. La liste des autorisés est affichée telle que configurée, et vous la lisez vous-même.

Comment voir quels ports sont configurés pour le 802.1X

Le 802.1X détermine si un équipement branché sur une prise murale a le droit d'accéder au réseau. NacTrack relit cette configuration sur les commutateurs, ce qui permet de voir où l'authentification des ports a réellement été déployée, et non où elle était prévue. C'est souvent l'écart entre les deux qui compte : un commutateur d'accès installé après le déploiement, ou un étage oublié, laisse ses ports ouverts à quiconque dispose d'un câble.

Nécessite: module: beta_testing, permission: view_inventory, data: has_dot1x, vendors: Cisco access switches; the fields come from interface configuration + beta_testing

- 1 La sécurité des ports se trouve sous Inventaire, à côté des vues d'interfaces, car ce qu'elle rapporte est de la configuration d'interface et non un produit de sécurité distinct.
- 2 Choisissez Access control. La page ne liste que les ports porteurs d'une configuration 802.1X : sa longueur constitue donc à elle seule la réponse sur l'avancement du déploiement.
- 3 Chaque ligne correspond à un port authentifié. La première colonne indique le commutateur : la parcourir vous dit lesquels participent et, tout aussi utile, lesquels n'apparaissent jamais.

Access control (802.1X)

Beta Feature under active development

AtlasWave Maroc De...

These are the ports configured for 802.1X or port-security in the device configurations. NacTrack does not collect authentication sessions, who authenticated, or port-security violation counters; those are live state, and collection is a periodic configuration snapshot. An empty column here means not collected, not zero.

802.1X PORTS96

MAB FALLBACK40

PORT-SECURITY PORTS12

DEVICES4

ShowAll

DEVICES	INTERFACE	DESCRIPTION	PORT CONTROL	HOST MODE	MAB	PORT-SECURITY	DATA VLAN
AWM-CAS-ACC-SW01	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/18	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/11	Casablanca user access port 11	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/12	Casablanca user access port 12	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/13	Casablanca user access port 13	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/14	Casablanca user access port 14	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/15	Casablanca user access port 15	auto	multi-domain	BYPASS	-	30
AWM-CAS-ACC-SW01	611/6/16	Casablanca user access port 16	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/17	Casablanca user access port 17	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/18	Casablanca user access port 18	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/19	Casablanca user access port 19	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/2	Casablanca user access port 02	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/20	Casablanca user access port 20	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/21	Casablanca user access port 21	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/22	Casablanca user access port 22	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/23	Casablanca user access port 23	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/24	Casablanca user access port 24	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/3	Casablanca user access port 03	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/4	Casablanca user access port 04	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/5	Casablanca user access port 05	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/6	Casablanca user access port 06	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/7	Casablanca user access port 07	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/8	Casablanca user access port 08	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/9	Casablanca user access port 09	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW02	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW02	611/6/18	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW03	611/6/11	Casablanca user access port 11	auto	multi-domain	-	-	10

Academy

- 4 Deux colonnes portent le sens. Port Control réglé sur auto est celle qui applique la règle : le port reste fermé tant que l'équipement connecté ne s'est pas authentifié. Host Mode indique combien d'équipements peuvent partager la prise, et multi-domain est le choix habituel pour un poste de travail : un ordinateur et un téléphone IP.

Access control (802.1X)

Beta feature under active development

AtlasWave Maroc De...

These are the ports configured for 802.1X or port-security in the device configurations. NacTrack does not collect authentication sessions, who authenticated, or port-security violation counters: those are live state, and collection is a periodic configuration snapshot. An empty column here means not collected, not zero.

802.1X PORTS: 96

MAB FALLBACK: 40

PORT-SECURITY PORTS: 12

DEVICES: 4

Show: All

DEVICES	INTERFACE	DESCRIPTION	PORT CONTROL	HOST MODE	MAB	PORT-SECURITY	DATA VLAN
AWM-CAS-ACC-SW01	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/18	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/11	Casablanca user access port 11	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/12	Casablanca user access port 12	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/13	Casablanca user access port 13	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/14	Casablanca user access port 14	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/15	Casablanca user access port 15	auto	multi-domain	BYPASS	-	30
AWM-CAS-ACC-SW01	611/6/16	Casablanca user access port 16	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/17	Casablanca user access port 17	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/18	Casablanca user access port 18	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/19	Casablanca user access port 19	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/2	Casablanca user access port 02	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/20	Casablanca user access port 20	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/21	Casablanca user access port 21	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/22	Casablanca user access port 22	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/23	Casablanca user access port 23	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/24	Casablanca user access port 24	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/3	Casablanca user access port 03	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/4	Casablanca user access port 04	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/5	Casablanca user access port 05	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/6	Casablanca user access port 06	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/7	Casablanca user access port 07	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/8	Casablanca user access port 08	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/9	Casablanca user access port 09	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW02	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW02	611/6/18	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW03	611/6/11	Casablanca user access port 11	auto	multi-domain	-	-	10

Academy

BON À SAVOIR

Il s'agit de configuration et non d'activité. Un port affiché en auto est paramétré pour exiger une authentification ; la page n'indique pas si quelque chose s'y est authentifié ni si un client a même essayé.

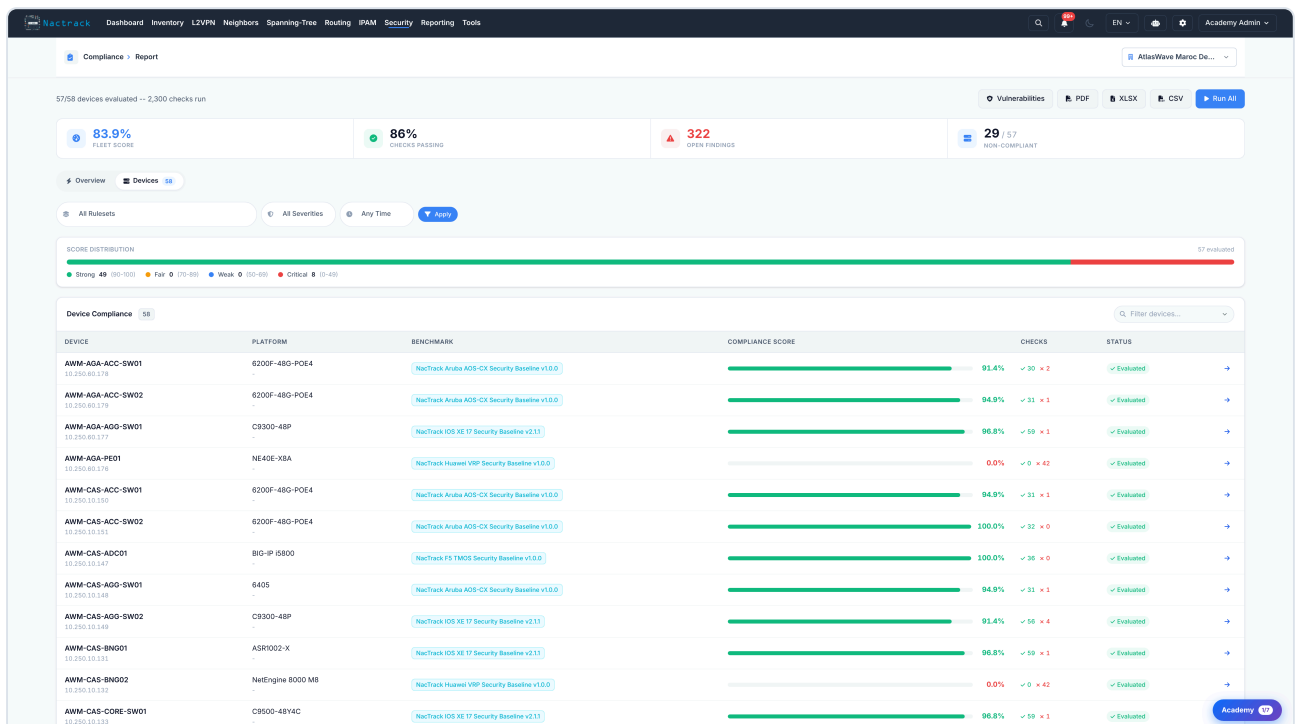
Un commutateur absent de la liste n'est pas forcément non protégé. Il peut s'agir d'un commutateur de coeur ou d'agrégation sans port utilisateur, où le 802.1X n'aurait rien à authentifier.

Comment vérifier si un équipement autorise encore Telnet

Telnet transmet les mots de passe en clair. La plupart des réseaux l'ont désactivé depuis des années, et c'est précisément pour cela que les équipements qui répondent encore sur le port 23 passent inaperçus : ce ne sont généralement pas ceux qui inquiètent. NacTrack évalue la configuration collectée par rapport à un référentiel de durcissement propre à la plateforme : la réponse vient donc de ce que l'équipement exécute réellement, et non de ce que le socle standard était censé contenir.

Nécessite: module: compliance, permission: view_audit, vendors: All benchmarked platforms; every shipped ruleset carries a Telnet check

- 1 La conformité se trouve sous Security, aux côtés de l'exposition aux CVE et du cycle de vie. Toutes trois répondent au même type de question : non pas ce que fait le réseau, mais dans quel état vous l'avez laissé.
- 2 Choisissez Compliance. Chaque équipement évalué apparaît avec le référentiel utilisé, un score, et le nombre de contrôles réussis.
- 3 Le rapport s'ouvre sur sa synthèse. Le tableau par équipement se trouve derrière l'onglet Devices, où se trouve le détail recherché.
- 4 Un score élevé n'est pas un certificat de bonne santé. C'est une moyenne pondérée : un équipement peut donc dépasser les quatre-vingt-dix pour cent tout en échouant à un contrôle de gravité haute. C'est précisément ce cas qu'il faut traquer, car personne ne regarde deux fois un équipement à quatre-vingt-quinze pour cent.



- 5 L'ouverture d'un équipement affiche tous les contrôles exécutés. Ce commutateur d'agrégation obtient près de quatre-vingt-quinze pour cent, et une ligne est marquée FAIL : le serveur Telnet est toujours actif.

Compliance > AWM-CAS-AGG-SW01

PDF Report

IP: 10.250.10.148 Model: 6405 Benchmark: NacTrack Aruba AOS-CX Security Baseline v1.0.0

Column visibility ▾ Excel CSV PDF Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-ARJ-11.ssh-server-vrf	Enable the SSH server on a VRF	HIGH Weight: 60 Profile: L1	PASS	ssh server vrf mgmt	Enable the SSH management server on a routing VRF.	-	-
NTC-ARJ-12.telnet-disabled	Disable the Telnet server	HIGH Weight: 60 Profile: L1	FAIL	Cleartext Telnet server is enabled	Disable the cleartext Telnet server; use SSH instead.	no telnet-server vrf default no telnet-server vrf mgmt	Reason (accepted risk) dd/mm/yyyy Waive
NTC-ARJ-13.https-server-vrf	Restrict the HTTPS/REST server to a VRF	MEDIUM Weight: 40 Profile: L2	PASS	https-server vrf mgmt	Expose the web/REST management interface only on a controlled VRF.	-	-
NTC-ARJ-14.no-plaintext-http	Disable the cleartext HTTP server	HIGH Weight: 60 Profile: L1	PASS	-	Disable the plaintext HTTP server; use HTTPS only.	-	-
NTC-ARJ-15.cli-session-timeout	Set CLI idle session timeout to 15 minutes or less	MEDIUM Weight: 40 Profile: L1	PASS	value=0.0	Time out idle management CLI sessions.	-	-
NTC-ARJ-16.banner-motd	Configure a login banner (message of the day)	LOW Weight: 1 Profile: L1	PASS	banner motd	Display an authorized-use notice before login.	-	-
NTC-ARJ-17.ssh-max-auth-attempts	Limit SSH authentication attempts	LOW Weight: 1 Profile: L1	PASS	value=3.0	Cap the number of SSH authentication attempts per connection.	-	-
NTC-ARJ-18.mgmt-vrf-separation	Bind SSH management to a dedicated management VRF	MEDIUM Weight: 40 Profile: L2	PASS	ssh server vrf mgmt	Run management services on the dedicated mgmt VRF, separated from data VRFs.	-	-
NTC-ARJ-21.aaa-login-remote	Authenticate management logins against remote AAA	HIGH Weight: 60 Profile: L1	PASS	aaa authentication login ssh group tacacs	Authenticate logins against a central AAA server, falling back to local.	-	-
NTC-ARJ-2.2.tacacs-server	Configure a TACACS+ server	MEDIUM Weight: 40 Profile: L1	PASS	tacacs-server host 10.0.0.5	Configure a TACACS+ authentication server with an encrypted key.	-	-

Showing 1 to 10 of 32 entries

Previous 1 2 3 4 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

Academy 10

- 6 La ligne porte plus qu'un verdict. Evidence indique ce qui a été trouvé dans la configuration, Recommendation explique pourquoi c'est important, et Fix fournit les commandes qui régleraient le problème. De quoi rédiger une demande de changement sans ouvrir l'équipement.

Compliance > AWM-CAS-AGG-SW01

PDF Report

IP: 10.250.10.148 Model: 6405 Benchmark: NacTrack Aruba AOS-CX Security Baseline v1.0.0

Column visibility ▾ Excel CSV PDF Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-ARJ-11.ssh-server-vrf	Enable the SSH server on a VRF	HIGH Weight: 60 Profile: L1	PASS	ssh server vrf mgmt	Enable the SSH management server on a routing VRF.	-	-
NTC-ARJ-12.telnet-disabled	Disable the Telnet server	HIGH Weight: 60 Profile: L1	FAIL	Cleartext Telnet server is enabled	Disable the cleartext Telnet server; use SSH instead.	no telnet-server vrf default no telnet-server vrf mgmt	Reason (accepted risk) dd/mm/yyyy Waive
NTC-ARJ-13.https-server-vrf	Restrict the HTTPS/REST server to a VRF	MEDIUM Weight: 40 Profile: L2	PASS	https-server vrf mgmt	Expose the web/REST management interface only on a controlled VRF.	-	-
NTC-ARJ-14.no-plaintext-http	Disable the cleartext HTTP server	HIGH Weight: 60 Profile: L1	PASS	-	Disable the plaintext HTTP server; use HTTPS only.	-	-
NTC-ARJ-15.cli-session-timeout	Set CLI idle session timeout to 15 minutes or less	MEDIUM Weight: 40 Profile: L1	PASS	value=0.0	Time out idle management CLI sessions.	-	-
NTC-ARJ-16.banner-motd	Configure a login banner (message of the day)	LOW Weight: 1 Profile: L1	PASS	banner motd	Display an authorized-use notice before login.	-	-
NTC-ARJ-17.ssh-max-auth-attempts	Limit SSH authentication attempts	LOW Weight: 1 Profile: L1	PASS	value=3.0	Cap the number of SSH authentication attempts per connection.	-	-
NTC-ARJ-18.mgmt-vrf-separation	Bind SSH management to a dedicated management VRF	MEDIUM Weight: 40 Profile: L2	PASS	ssh server vrf mgmt	Run management services on the dedicated mgmt VRF, separated from data VRFs.	-	-
NTC-ARJ-21.aaa-login-remote	Authenticate management logins against remote AAA	HIGH Weight: 60 Profile: L1	PASS	aaa authentication login ssh group tacacs	Authenticate logins against a central AAA server, falling back to local.	-	-
NTC-ARJ-2.2.tacacs-server	Configure a TACACS+ server	MEDIUM Weight: 40 Profile: L1	PASS	tacacs-server host 10.0.0.5	Configure a TACACS+ authentication server with an encrypted key.	-	-

Showing 1 to 10 of 32 entries

Previous 1 2 3 4 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

Academy 10

BON À SAVOIR

Ceci lit la configuration, pas l'accessibilité. Un équipement dont le serveur Telnet est actif peut rester injoignable sur le port 23 parce qu'un pare-feu ou une ACL de gestion le bloque. Le constat dit que la porte n'est pas verrouillée, pas que l'on puisse y accéder.

Le verdict n'est pas plus récent que la dernière collecte de configuration. Un équipement durci ce matin reste en échec tant qu'il n'a pas été collecté et réévalué.

Comment repérer les équipements utilisant des communautés SNMP par défaut ou en version 1 et 2c

Une communauté SNMP est un mot de passe transmis en clair, et les versions 1 et 2c n'offrent aucune autre protection. Les communautés nommées public et private sont pires encore : ce sont les deux premières que l'on essaie. Cela survit rarement par négligence, plutôt par héritage : un outil de supervision a eu besoin d'un accès en lecture il y a des années, la communauté a été déployée sur toute la flotte, et rien depuis n'a donné de raison d'y revenir.

Nécessite: module: compliance, permission: view_audit, vendors: All benchmarked platforms; the wording of the check differs by vendor

- 1 Ouvrez Security puis Compliance. SNMP est évalué par le même référentiel propre à la plateforme qui couvre Telnet et le reste du plan de gestion.
- 2 Ce commutateur spine échoue à deux contrôles, tous deux relatifs à SNMP. Ce sont volontairement deux questions distinctes : l'une porte sur l'usage d'un nom de communauté par défaut, l'autre sur l'activation même des versions 1 ou 2c.

The screenshot displays the NacTrack Security Compliance interface. The top navigation bar includes links for Dashboard, Inventory, L2VPN, Neighbors, Spanning-Tree, Routing, IPAM, Security, Reporting, and Tools. The main content area shows a compliance check for the device 10.250.10.136 (Model 7280SR3K-48YC8) against the NacTrack Arista EOS Security Baseline v4.0.0. The interface includes a table with columns for Code, Title, Severity, Status, Evidence / Details, Recommendation, Fix, and Waiver. The table lists 10 security checks, all of which are marked as 'PASS'. The bottom section shows 'Recent Evaluation Jobs' with a message: 'No compliance jobs have been recorded yet.'

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-EOS-11.api-tls	eAPI http-commands must use HTTPS/TLS	MEDIUM Weight: 40 Profile: L1	PASS	management api http-commands: protocol https	Serve eAPI over TLS only.	-	-
NTC-EOS-11.console-idle-timeout	Console session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management console: value=15.0	Bound idle console sessions.	-	-
NTC-EOS-11.http-disabled	Disable the cleartext HTTP management interface	HIGH Weight: 80 Profile: L1	PASS	no protocol http	Disable plaintext HTTP, keep HTTPS only.	-	-
NTC-EOS-11.login-banner	Present a login banner	LOW Weight: 1 Profile: L1	PASS	banner login	Display an authorized-use banner.	-	-
NTC-EOS-11.no-telnet	Disable the Telnet management server	HIGH Weight: 80 Profile: L1	PASS	no ip telnet server	Disable the cleartext Telnet server.	-	-
NTC-EOS-11.ssh-enabled	Enable the SSH management server	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: no shutdown	Bring up the SSH management service.	-	-
NTC-EOS-11.ssh-idle-timeout	SSH session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: value=10.0	Bound idle SSH sessions.	-	-
NTC-EOS-12.aaa-auth-login	Configure AAA login authentication	HIGH Weight: 80 Profile: L1	PASS	aaa authentication login	Define a login authentication method.	-	-
NTC-EOS-12.aaa-login-remote-group	Login authentication uses a TACACS+/RADIUS group	MEDIUM Weight: 40 Profile: L1	PASS	aaa authentication login default group tacacs+	Authenticate against a central AAA server with local fallback.	-	-
NTC-EOS-12.aaa-root	aaa root protected by a secret	MEDIUM Weight: 40 Profile: L1	PASS	aaa root secret	Set a secret on the root account.	-	-

Showing 1 to 10 of 20 entries

Previous 1 2 3 Next

Recent Evaluation Jobs
No compliance jobs have been recorded yet.

Academy 10

- 3 Chaque colonne dispose de son propre filtre. Saisir FAIL sous Status réduit le tableau à ce qui ne va pas, ce qui compte ici : la plupart des contrôles de cet équipement passent et rempliraient plusieurs pages avant d'arriver aux deux qui échouent.

Compliance > AWM-CAS-DC-SP02

PDF Report

IP: 10.250.10.136 Model: 7280SR3K-48YC8 Benchmark: NacTrack Arista EOS Security Baseline v4.0.0

Column visibility Excel CSV PDF Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-EOS-11.api-tls	eAPI http-commands must use HTTPS/TLS	MEDIUM Weight: 40 Profile: L1	PASS	management api http-commands: protocol https	Serve eAPI over TLS only.	-	-
NTC-EOS-11.console-idle-timeout	Console session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management console: value=15.0	Bound idle console sessions.	-	-
NTC-EOS-11.http-disabled	Disable the cleartext HTTP management interface	HIGH Weight: 80 Profile: L1	PASS	no protocol http	Disable plaintext HTTP, keep HTTPS only.	-	-
NTC-EOS-11.login-banner	Present a login banner	LOW Weight: 1 Profile: L1	PASS	banner login	Display an authorized-use banner.	-	-
NTC-EOS-11.no-telnet	Disable the Telnet management server	HIGH Weight: 80 Profile: L1	PASS	no ip telnet server	Disable the cleartext Telnet server.	-	-
NTC-EOS-11.ssh-enabled	Enable the SSH management server	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: no shutdown	Bring up the SSH management service.	-	-
NTC-EOS-11.ssh-idle-timeout	SSH session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: value=10.0	Bound idle SSH sessions.	-	-
NTC-EOS-12.aaa-auth-login	Configure AAA login authentication	HIGH Weight: 80 Profile: L1	PASS	aaa authentication login	Define a login authentication method.	-	-
NTC-EOS-12.aaa-login-remote-group	Login authentication uses a TACACS+/RADIUS group	MEDIUM Weight: 40 Profile: L1	PASS	aaa authentication login default group=tacacs+	Authenticate against a central AAA server with local fallback.	-	-
NTC-EOS-12.aaa-root	aaa root protected by a secret	MEDIUM Weight: 40 Profile: L1	PASS	aaa root secret	Set a secret on the root account.	-	-

Showing 1 to 10 of 29 entries

Previous 1 2 3 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

Academy

- 4 Le tableau se filtre à la frappe. Un instant plus tard, seules les lignes en échec restent.

- 5 La distinction compte au moment de corriger. Renommer une communauté satisfait le premier contrôle et laisse le second en échec, car le trafic reste non authentifié et non chiffré. Seul le passage en version 3 règle les deux.

Compliance > AWM-CAS-DC-SP02

PDF Report

IP: 10.250.10.136 Model: 7280SR3K-48YC8 Benchmark: NacTrack Arista EOS Security Baseline v4.0.0

Column visibility Excel CSV PDF Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-EOS-13.no-default-community	No default SNMP community (public/private)	HIGH Weight: 80 Profile: L1	FAIL	Guessable SNMP community present	Remove default communities.	configure no snmp-server community public no snmp-server community private end	Reason (accepted risk) dt/mn/yyyy Waiver
NTC-EOS-13.no-v1v2-community	No SNMP v1/v2c communities (v3 only)	MEDIUM Weight: 40 Profile: L2	FAIL	SNMP v1v2c community configured	Drop all communities and use SNMPv3.	configure no snmp-server community comm-ent	Reason (accepted risk) dt/mn/yyyy Waiver

Showing 1 to 2 of 2 entries (Filtered from 29 total entries)

Previous 1 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

BON À SAVOIR

Un équipement sans aucune configuration SNMP réussit les deux contrôles. Réussir signifie donc "non exposé de cette manière" et non "supervisé de façon sûre" : le référentiel ne distingue pas un équipement volontairement durci d'un équipement que personne n'a jamais configuré.

Les communautés sont des identifiants. NacTrack signale l'existence d'une communauté faible sans afficher sa valeur dans les preuves : le rapport peut donc être partagé sans divulguer ce qu'il a trouvé.

Comment lire la posture d'accès de gestion d'un équipement

L'exposition de gestion n'est pas un réglage unique. C'est la somme des services qui répondent, de leur chiffrement, de leur confinement dans un VRF de gestion, de l'authentification centralisée à la connexion, et de la fermeture des sessions inactives. Pris isolément, ces contrôles ressemblent à de l'entretien. Lus ensemble pour un même équipement, ils décrivent la manière dont quelqu'un entrerait, et c'est cette lecture qu'il faut apprendre.

Nécessite: module: compliance, permission: view_audit, vendors: All benchmarked platforms; check names and counts differ by vendor

- 1
- Ouvrez Security puis Compliance, et triez par score. Les scores les plus bas correspondent aux équipements dont le plan de gestion n'a jamais été durci, plutôt qu'à une dérive isolée.
- 2
- Celui-ci échoue à tous les contrôles exécutés. Ce schéma est caractéristique : ce n'est pas un équipement qui a dérivé, c'est un équipement qui n'a jamais été aligné sur le socle standard.

Compliance

AWM-CAS-BNG02

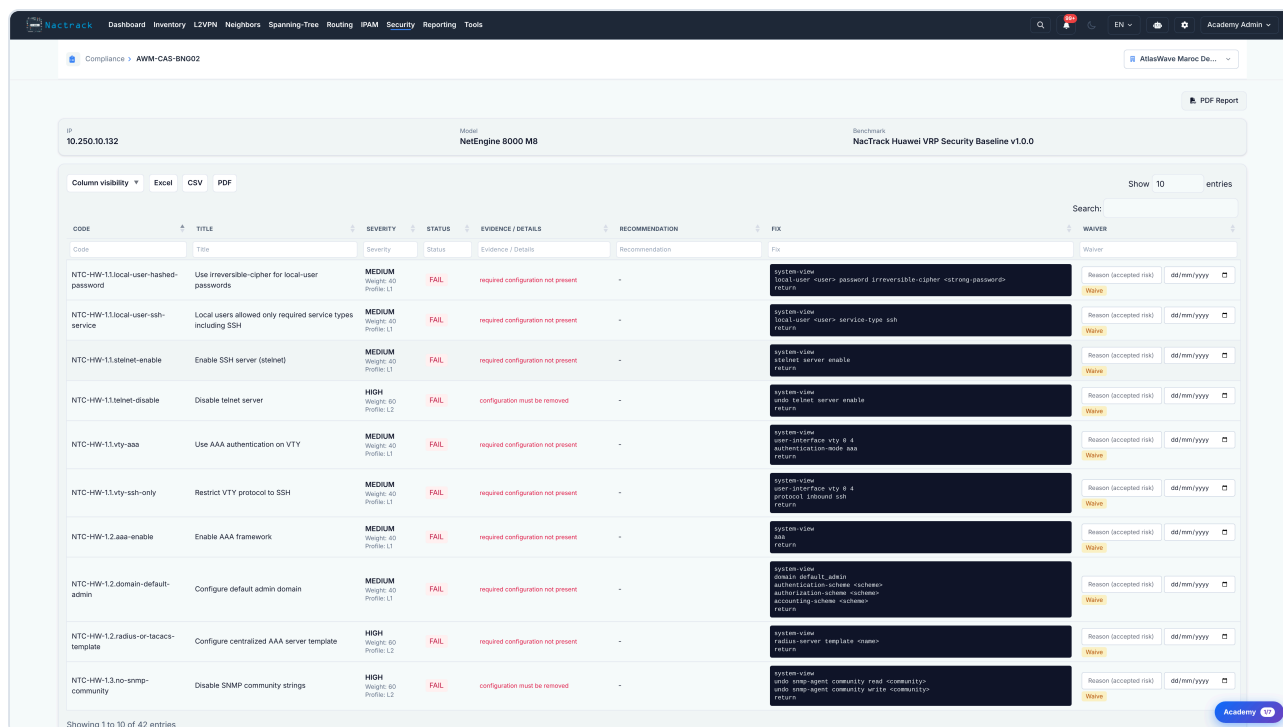
PDF Report

IP	Model	Benchmark					
10.250.10.132	NetEngine 8000 MB	NacTrack Huawei VRP Security Baseline v1.0.0					
Column visibility	Excel	CSV	PDF				
Search:			Show 10 entries				
CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
Code	Title	Severity	Status	Evidence / Details	Recommendation	Fix	Waiver
NTC-HW-1.1.local-user-has-hashed-password	Use irreversible-cipher for local-user passwords	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view local-user <user> password irreversible-cipher <strong-password> return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.1.local-user-ssh-service	Local users allowed only required service types including SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view local-user <user> service-type ssh return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.1.telnet-enable	Enable SSH server (stelsht)	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view stelnet server enable return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.1.telnet-disable	Disable telnet server	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system-view undo telnet server enable return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.1.vty-aaa	Use AAA authentication on VTY	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view user-interface vty 0 4 authentication-mode aaa return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.1.vty-ssh-only	Restrict VTY protocol to SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view user-interface vty 0 4 protocol ssh return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.2.aaa-enable	Enable AAA framework	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view aaa return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.2.domain-default-admin	Configure default admin domain	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view domain default-adom authentication-scheme <scheme> authorization-scheme <scheme> accounting-scheme <scheme> return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.2.radius-or-tacacs-template	Configure centralized AAA server template	HIGH Weight: 60 Profile: L2	FAIL	required configuration not present	-	system-view radius-server template <name> return	Reason (accepted risk) dd/mm/yyyy Waive
NTC-HW-1.3.no-snmp-community	Disable SNMP community strings	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system-view undo snmp-agent community read <community> undo snmp-agent community write <community> return	Reason (accepted risk) dd/mm/yyyy Waive

Showing 1 to 10 of 42 entries

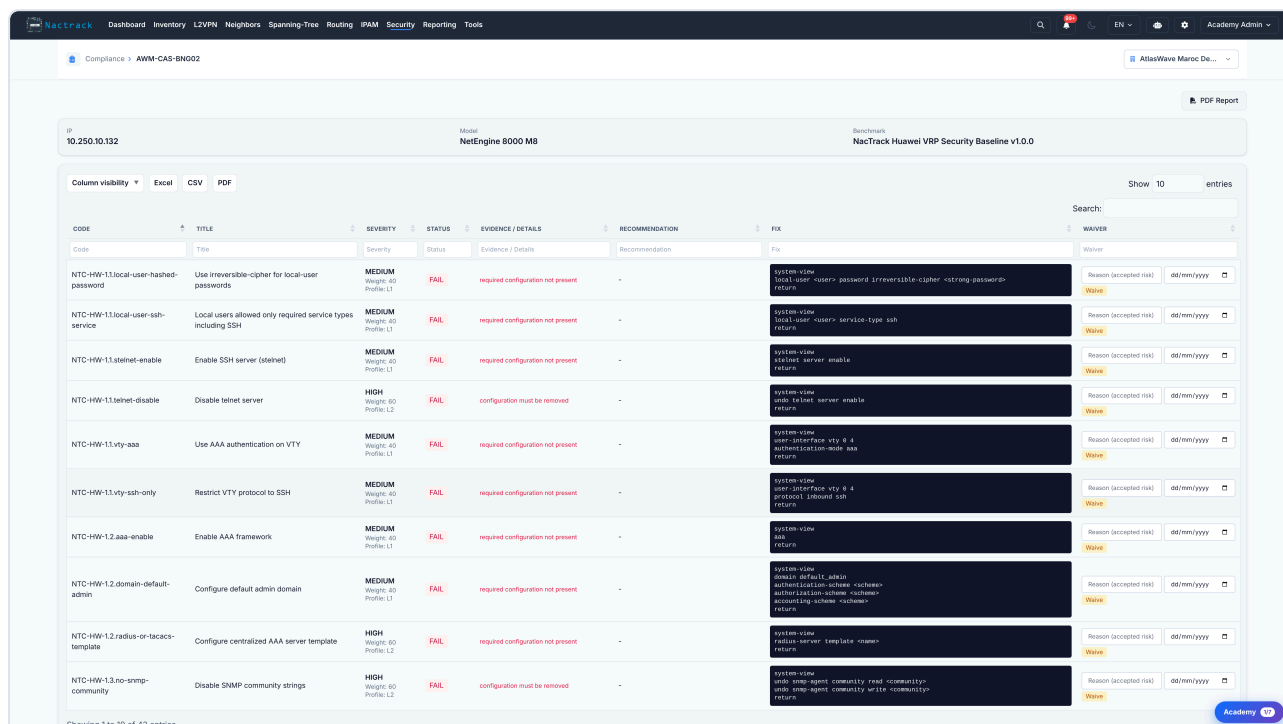
Academy

- 3 Notez le sens de ce contrôle. Il ne demande pas de désactiver un service : il indique que le serveur SSH devrait être actif et ne l'est pas. Combinez cela au serveur Telnet actif et vous tenez toute l'histoire : le seul accès à cet équipement est celui qui n'est pas chiffré.



CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	Search:	WAVER
Code	Title	Severity	Status	Evidence / Details	Recommendation	Fix		Waiver
NTC-HW-1.1.local-user-has-hashed-password	Use irreversible-cipher for local-user passwords	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view local-user <user> password irreversible-cipher <strong password> return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.local-user-ssh-service	Local users allowed only required service types including SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view local-user <user> service-type ssh return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.telnet-enable	Enable SSH server (stelnet)	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view stelnet server enable return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.telnet-disable	Disable telnet server	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system-view undo telnet server enable return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.vty-aaa	Use AAA authentication on VTY	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view user-interface vty 0 4 authentication-mode aaa return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.vty-ssh-only	Restrict VTY protocol to SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view user-interface vty 0 4 protocol inbound ssh return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.2.aaa-enable	Enable AAA framework	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view aaa return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.2.domain-default-admin	Configure default admin domain	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view domain default-admin authentication-scheme <scheme> authorization-scheme <scheme> accounting-scheme <scheme> return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.2.radius-or-tacacs-template	Configure centralized AAA server template	HIGH Weight: 60 Profile: L2	FAIL	required configuration not present	-	system-view radius-server template <name> return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.3.no-snmp-community	Disable SNMP community strings	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system-view undo snmp-agent community read <community> undo snmp-agent community write <community> return	Reason (accepted risk)	dd/mm/yyyy

- 4 Les lignes de terminal le confirment. Ce contrôle exige que les sessions VTY soient limitées à SSH, et il est en échec : les lignes acceptent donc tout ce que l'équipement propose. Trois constats mineurs pris isolément viennent de décrire un chemin d'accès complet.



CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	Search:	WAVER
Code	Title	Severity	Status	Evidence / Details	Recommendation	Fix		Waiver
NTC-HW-1.1.local-user-has-hashed-password	Use irreversible-cipher for local-user passwords	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view local-user <user> password irreversible-cipher <strong password> return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.local-user-ssh-service	Local users allowed only required service types including SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view local-user <user> service-type ssh return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.telnet-enable	Enable SSH server (stelnet)	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view stelnet server enable return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.telnet-disable	Disable telnet server	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system-view undo telnet server enable return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.vty-aaa	Use AAA authentication on VTY	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view user-interface vty 0 4 authentication-mode aaa return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.1.vty-ssh-only	Restrict VTY protocol to SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view user-interface vty 0 4 protocol inbound ssh return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.2.aaa-enable	Enable AAA framework	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view aaa return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.2.domain-default-admin	Configure default admin domain	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system-view domain default-admin authentication-scheme <scheme> authorization-scheme <scheme> accounting-scheme <scheme> return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.2.radius-or-tacacs-template	Configure centralized AAA server template	HIGH Weight: 60 Profile: L2	FAIL	required configuration not present	-	system-view radius-server template <name> return	Reason (accepted risk)	dd/mm/yyyy
NTC-HW-1.3.no-snmp-community	Disable SNMP community strings	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system-view undo snmp-agent community read <community> undo snmp-agent community write <community> return	Reason (accepted risk)	dd/mm/yyyy

BON À SAVOIR

Un référentiel est un avis livré sur une plateforme, pas la politique de votre organisation. Un équipement exécutant volontairement un service autorisé par votre standard restera signalé en échec tant que le contrôle n'est pas levé.

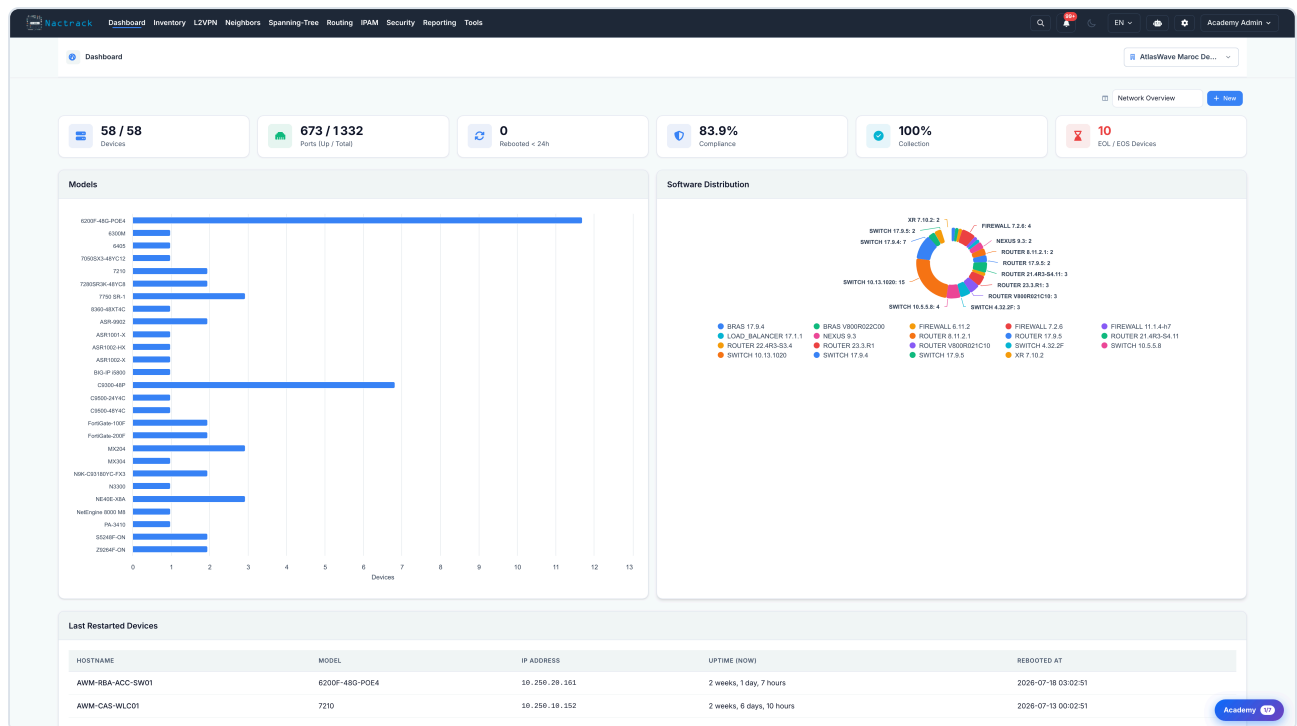
Le nombre de contrôles n'est pas comparable d'un constructeur à l'autre. Le référentiel d'une plateforme peut exécuter trente contrôles et un autre soixante : un score plus faible ne signifie donc pas automatiquement un équipement plus mauvais. Comparez un équipement au socle de sa propre plateforme.

Comment trouver quel switch est pont racine pour chaque VLAN

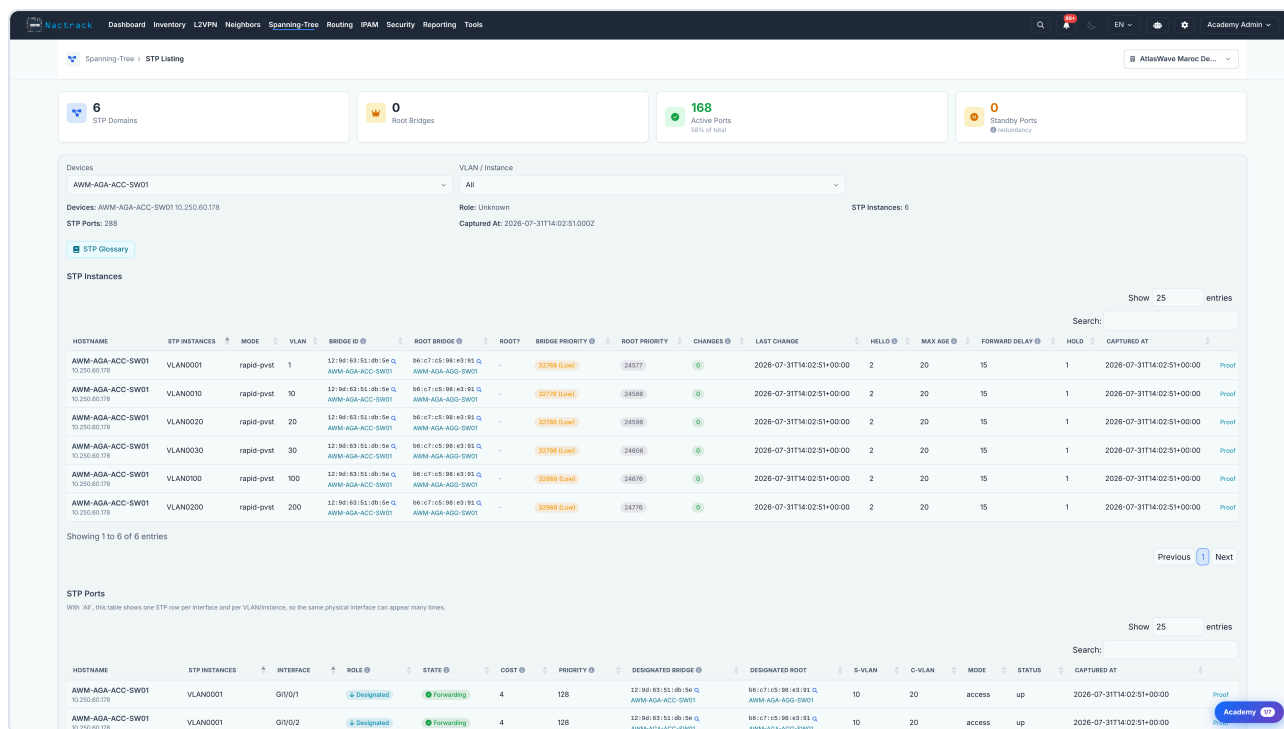
Le spanning tree décide quels liens transmettent et lesquels restent en attente, et il le décide à partir du pont racine. Si la racine n'est pas là où vous l'avez conçue, le trafic emprunte un chemin que vous n'avez pas choisi. La liste STP indique, pour chaque switch et chaque VLAN, quel pont il considère comme racine : vous vérifiez tout le parc d'un seul coup d'oeil.

Nécessite: module: stp, permission: view_stp, vendors: Cisco and Huawei switches only

- 1 Depuis le tableau de bord. Le spanning tree possède son propre menu de premier niveau, car c'est un plan de contrôle de niveau 2 à part entière et non une propriété d'un équipement.



- 2 Ouvrez Spanning-Tree et choisissez STP Listing. Le tableau du haut donne une ligne par switch et par VLAN : Bridge ID est l'identité propre du switch, et Root Bridge celui qu'il considère actuellement comme racine. Les deux sont affichés en adresse plus nom, ce qui évite toute traduction de MAC.



Spanning-Tree > STP Listing

6 STP Domains, 0 Root Bridges, 168 Active Ports (54% of total)

Devices: AWM-AGA-ACC-SW01 10.250.60.178, STP Ports: 288, STP Instances: 6

STP Glossary

STP Instances

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT7	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32778 (Low)	24586	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24606	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24676	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

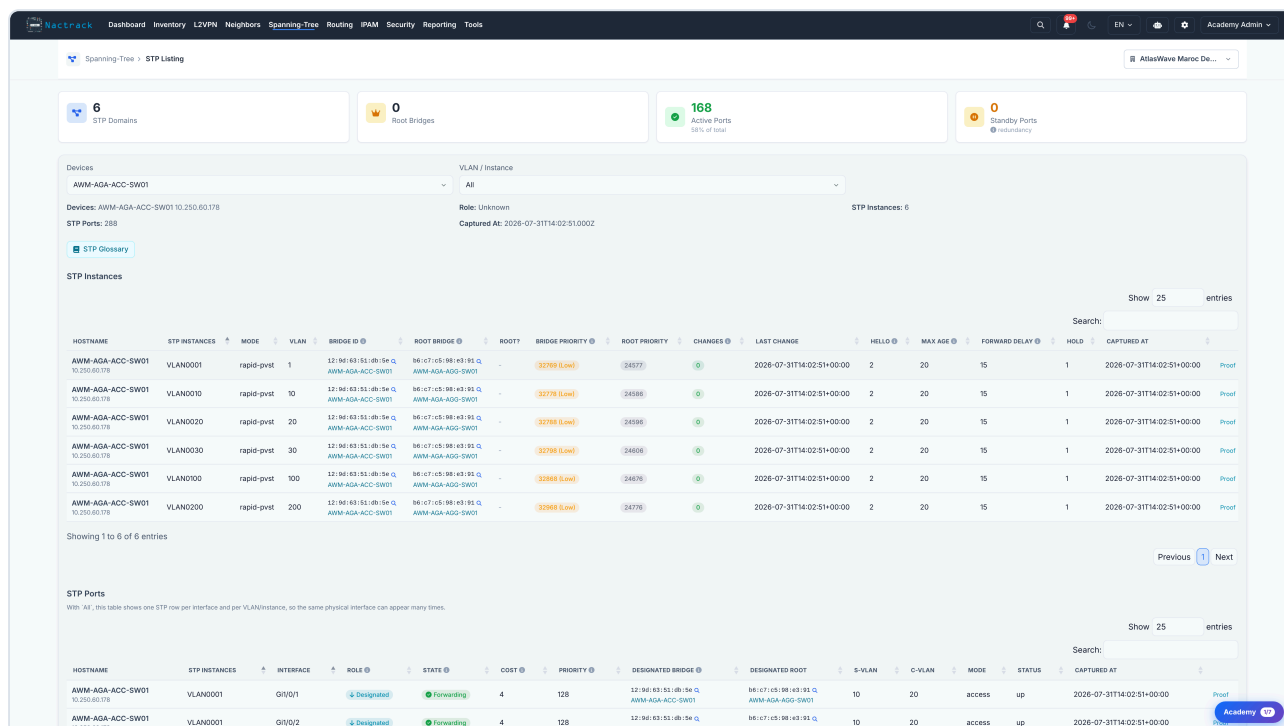
Showing 1 to 6 of 6 entries

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/1	Designated	Forwarding	4	128	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/2	Designated	Forwarding	4	128	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

- 3 Parcourez la colonne Root Bridge. Dans un campus sain, tous les VLAN devraient désigner le même switch d'agrégation, et Root Priority indique si cela a été configuré volontairement ou remporté par hasard sur une adresse départageante.



Spanning-Tree > STP Listing

6 STP Domains, 0 Root Bridges, 168 Active Ports (54% of total)

Devices: AWM-AGA-ACC-SW01 10.250.60.178, STP Ports: 288, STP Instances: 6

STP Glossary

STP Instances

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT7	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32778 (Low)	24586	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24606	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24676	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

Showing 1 to 6 of 6 entries

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/1	Designated	Forwarding	4	128	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/2	Designated	Forwarding	4	128	12:86:63:51:db:5a Q AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

BON À SAVOIR

Une priorité laissée par défaut signifie que la racine a été déterminée par l'adresse MAC la plus basse et non par conception. Elle changera le jour où ce switch sera remplacé.

Le spanning tree n'est collecté que sur les switchs Cisco et Huawei, et il est retiré des routeurs. Une couche d'accès Aruba ou Dell n'apparaîtra pas ici, même si elle exécute bien du spanning tree.

Comment trouver quels ports le spanning tree bloque

Un port bloquant n'est pas une panne. C'est le spanning tree qui fait son travail, en gardant un lien redondant en réserve pour éviter toute boucle. Ce qui compte, c'est de savoir si les ports qu'il a choisi de bloquer sont ceux que vous auriez choisis, car un lien bloqué du mauvais côté fait passer le trafic par le chemin le plus long, tous les jours, sans que personne le remarque.

Nécessite: module: stp, permission: view_stp, vendors: Cisco and Huawei switches only

- 1 Ouvrez Spanning-Tree puis STP Listing. C'est le tableau du bas qui nous intéresse : chaque port participant au spanning tree, sur chaque switch, avec le rôle qui lui a été attribué et l'état dans lequel il s'est stabilisé.

Spanning-Tree > STP Listing

6 STP Domains

0 Root Bridges

168 Active Ports (50% of total)

0 Standby Ports (0 redundancy)

Devices: AWM-AGA-ACC-SW01

VLAN / Instance: All

Role: Unknown

STP Instances: 6

Captured At: 2026-07-31T14:02:51.000Z

STP Glossary

STP Instances

Show 25 entries

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT?	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24586	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24606	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	-	32688 (Low)	24676	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	-	32688 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

Showing 1 to 6 of 6 entries

Previous 1 Next

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

Show 25 entries

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/01	Designated	Forwarding	4	128	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/02	Designated	Forwarding	4	128	12:96:63:15:db:5e Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:91 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

- 2 Deux colonnes portent la réponse. Role est la fonction attribuée par le spanning tree, et State ce que le port fait réellement. Un port en rôle Alternate et en état Blocking est un secours sain : il a un chemin vers la racine mais un meilleur existe, alors il attend.

Spanning-Tree > STP Listing

6 STP Domains

0 Root Bridges

168 Active Ports
50% of total

0 Standby Ports
0 redundancy

Devices: AWM-AGA-ACC-SW01
STP Ports: 288

Role: Unknown
Captured At: 2026-07-31T14:02:51.000Z

STP Instances: 6

STP Glossary

STP Instances

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	-	32778 (Low)	24585	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	-	32785 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	-	32795 (Low)	24605	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	-	32868 (Low)	24676	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	-	32868 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

Showing 1 to 6 of 6 entries

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	G1/0/1	Designated	Forwarding	4	128	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	G1/0/2	Designated	Forwarding	4	128	12:8d:63:15:db:1a Q AWM-AGA-ACC-SW01	86:c7:c5:98:k3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

BON À SAVOIR

Sur un switch d'accès, la plupart des ports affichent Disabled plutôt que Forwarding ou Blocking. Ce n'est pas le spanning tree qui les rejette : c'est simplement que rien n'y est branché.

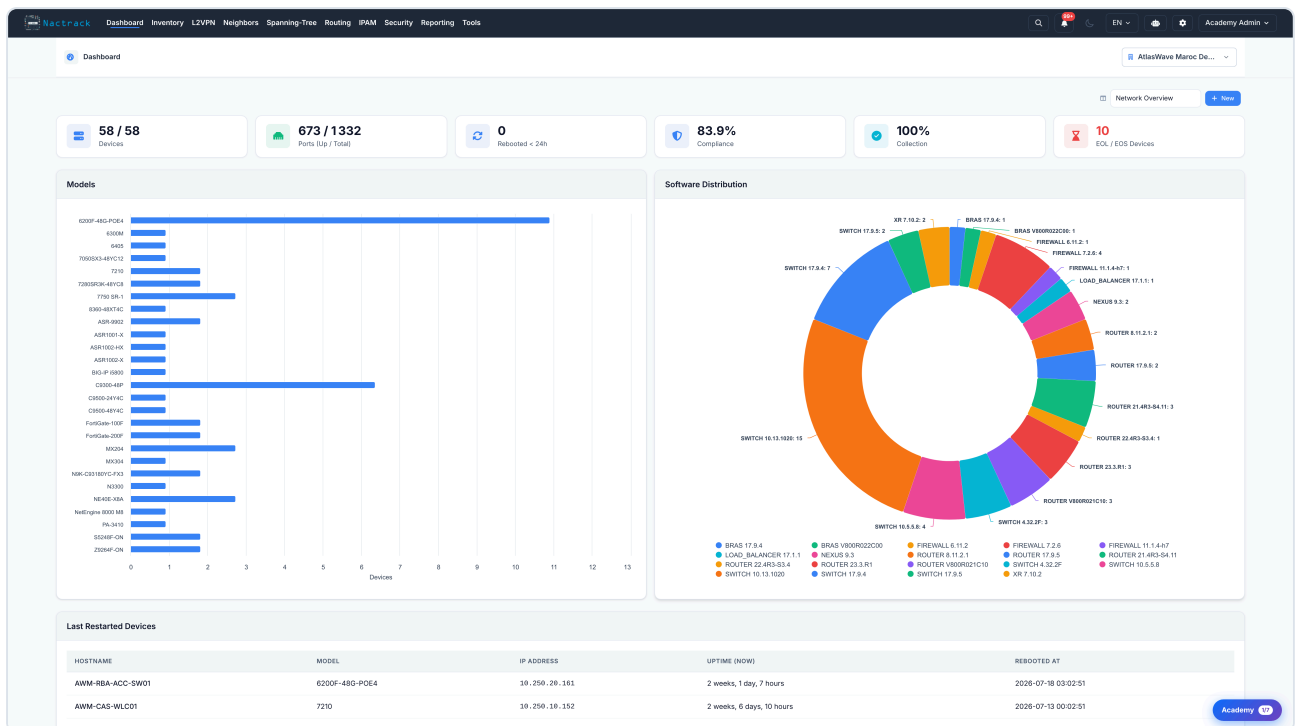
Il s'agit de l'état à la dernière collecte et non d'un flux en direct. Un port qui a convergé différemment depuis affichera encore l'état qu'il avait lors de la collecte.

Comment vérifier si BPDU Guard est activé sur les ports d'accès

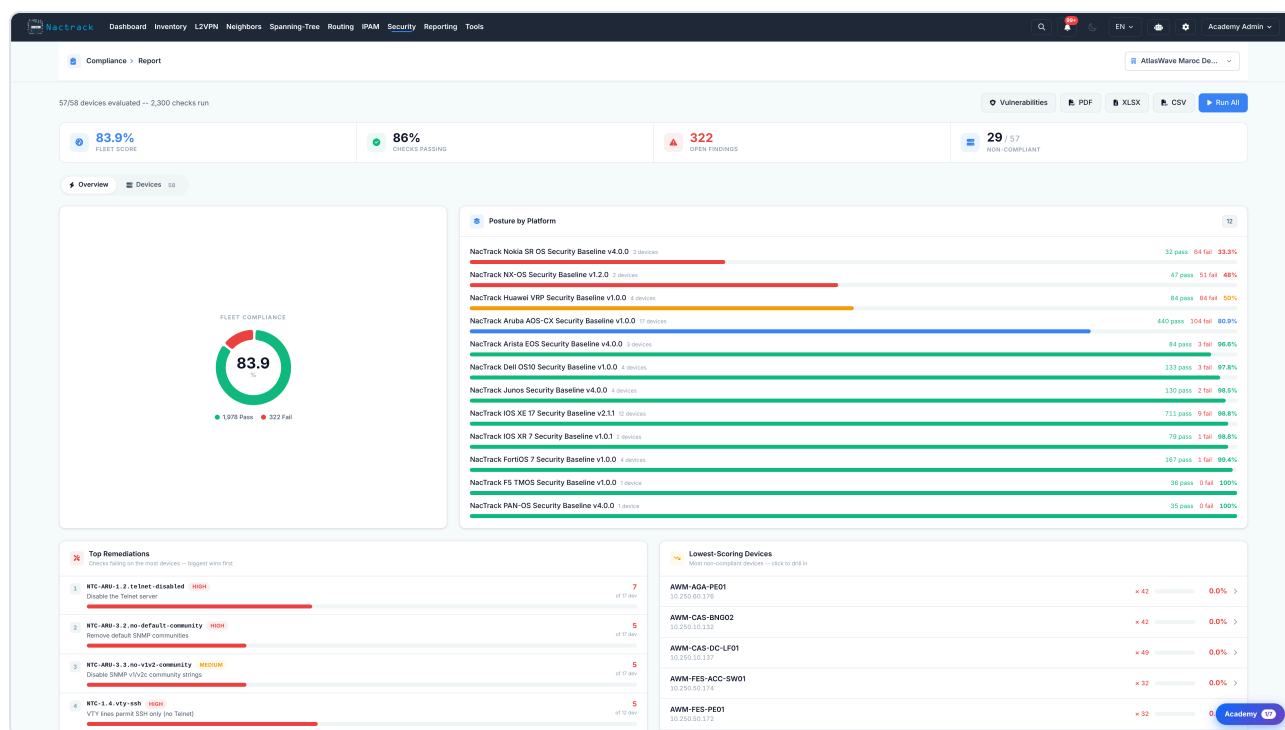
BPDU Guard désactive un port dès qu'un switch apparaît là où seuls des terminaux devraient se trouver : c'est ce qui empêche quelqu'un de brancher un switch de bureau sur une prise murale et de réorganiser votre spanning tree. NacTrack ne le lit pas dans l'état courant : il vérifie la configuration au regard d'une règle de référence. La réponse se trouve donc dans Compliance et non dans la page STP.

Nécessite: module: compliance, permission: view_audit, vendors: Aruba AOS-CX, Cisco NX-OS and Dell OS10 only

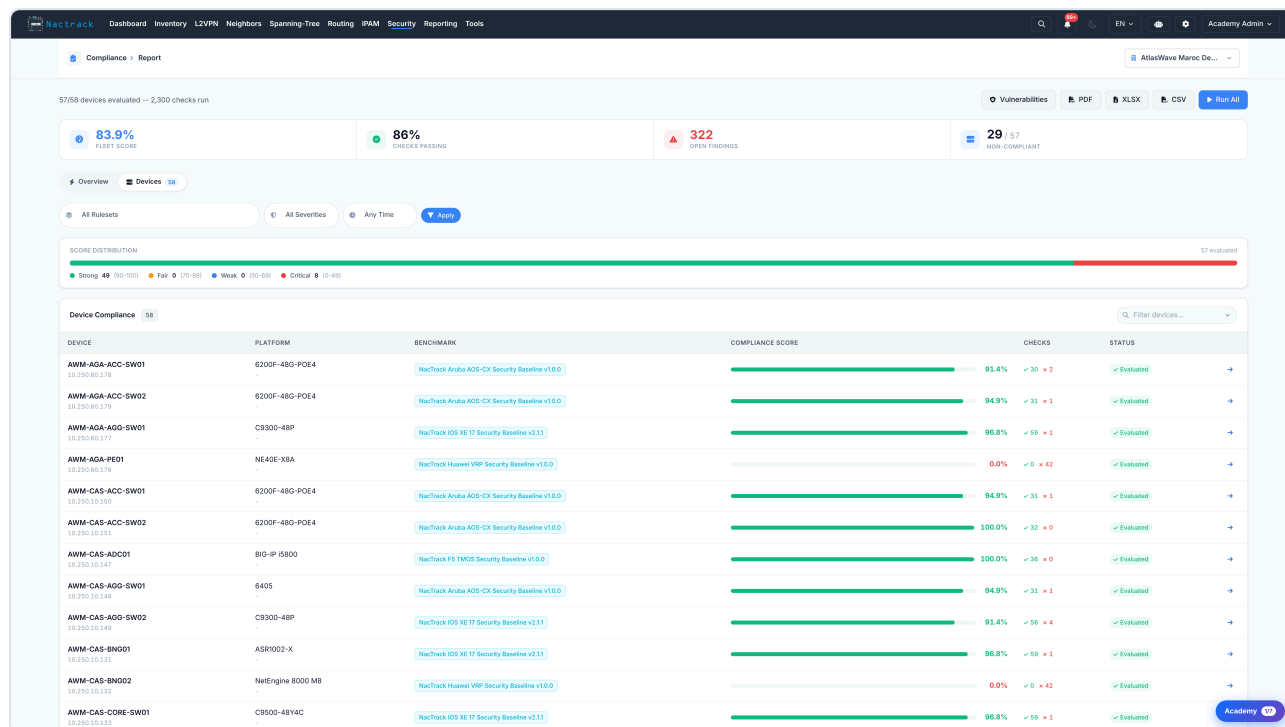
- 1 Depuis le tableau de bord. C'est une question de configuration et non d'état courant : elle relève donc de Security, avec le reste du travail de conformité.



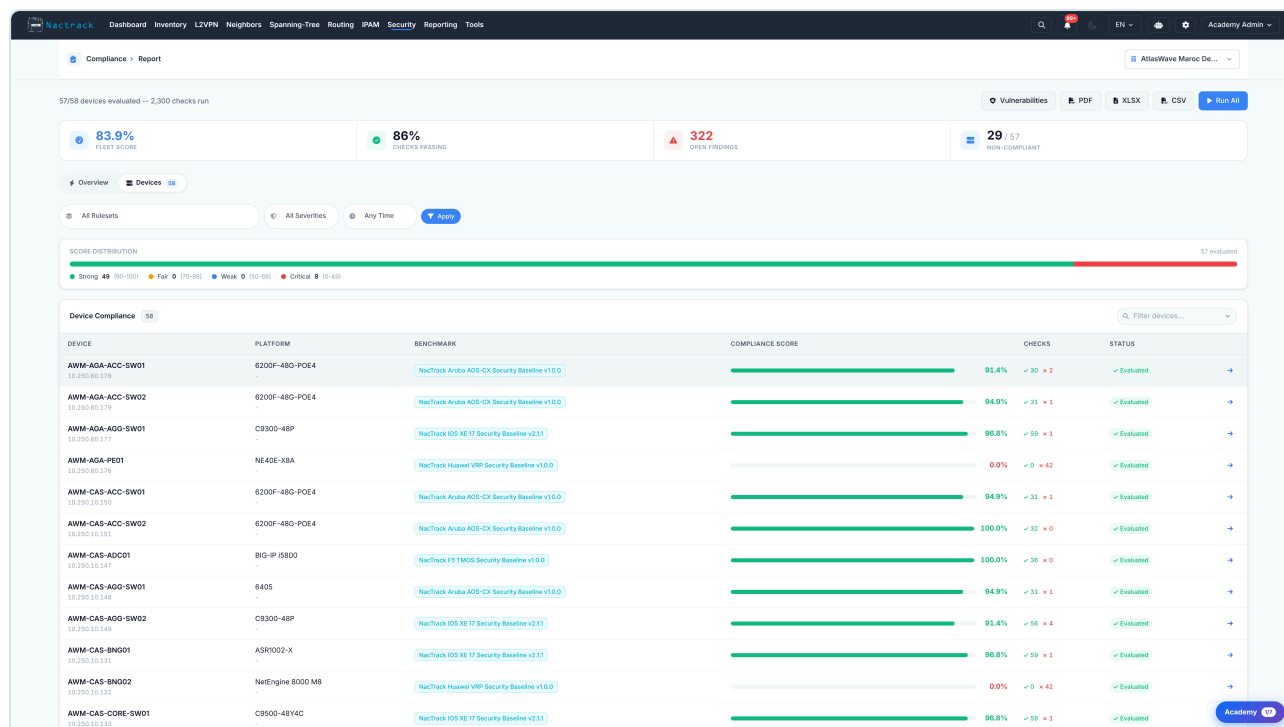
- 2 Ouvrez Security et choisissez Compliance. La page s'ouvre sur Overview, la synthèse du parc : la posture de tous les équipements, sans le détail d'aucun.



- 3 Passez sur l'onglet Devices. Chaque équipement évalué est maintenant listé avec son score et le nombre de contrôles appliqués. Le compteur à côté du nom de l'onglet vous l'indique avant même de cliquer.



- 4 Ouvrez un équipement pour voir ses contrôles individuels. La règle BPDU Guard y figure nommément, réussie ou échouée, avec la ligne de configuration qui a tranché. C'est cette ligne que vous porteriez à une demande de changement.



BON À SAVOIR

Seules trois règles couvrent BPDU Guard, une pour Aruba AOS-CX, une pour Cisco NX-OS et une pour Dell OS10. Un switch d'accès Cisco IOS ou IOS-XE n'est pas contrôlé du tout : un bon score ne signifie donc pas que toute la périphérie est protégée.

La conformité lit du texte de configuration. Elle peut confirmer que la commande est présente ; elle ne peut pas dire que le port a réellement bloqué quoi que ce soit.

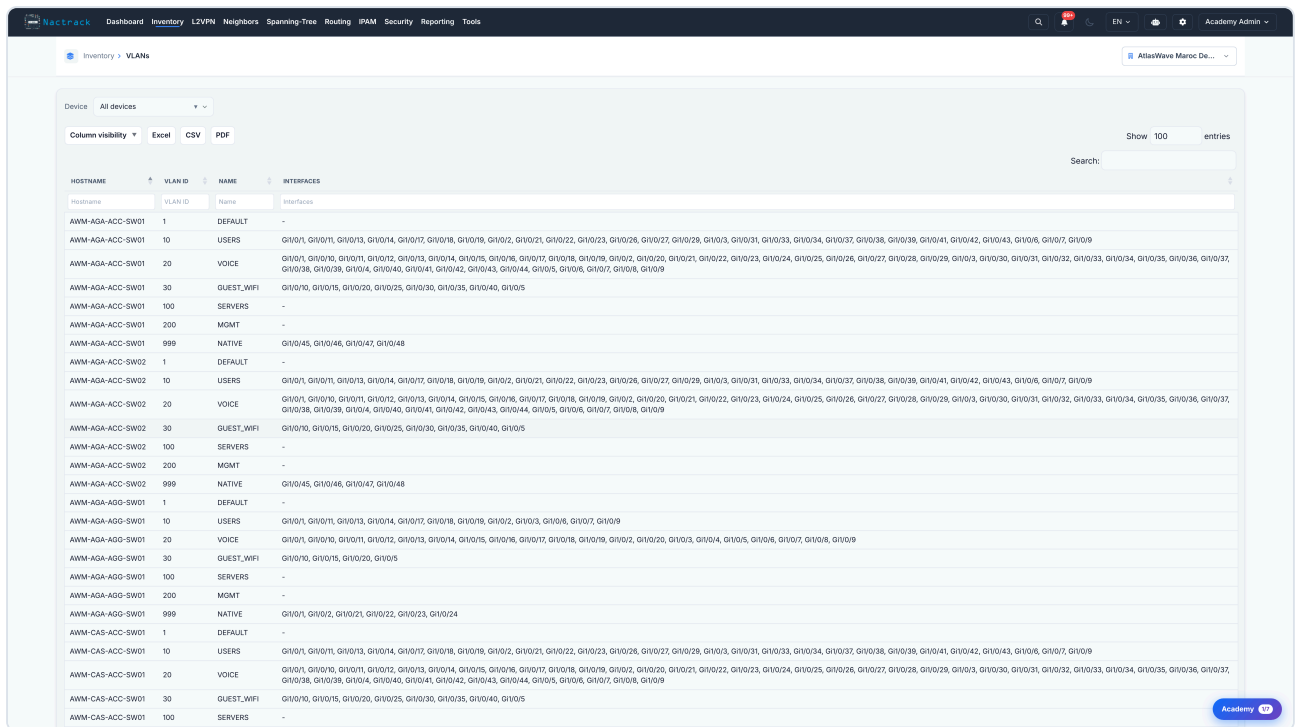
Root Guard est une fonction différente, que NacTrack ne contrôle nulle part. Ne considérez pas qu'un BPDU Guard conforme la couvre.

Comment savoir si un VLAN a encore des ports sur un switch

Les VLAN survivent aux besoins qui les ont créés. Avant d'en supprimer un, la bonne question n'est pas "ce VLAN est-il utilisé" dans l'absolu mais "ce switch a-t-il encore des ports dedans", car c'est une question à laquelle on peut répondre et c'est elle qui détermine si la suppression casse quelque chose localement.

Nécessite: module: inventory, permission: view_inventory

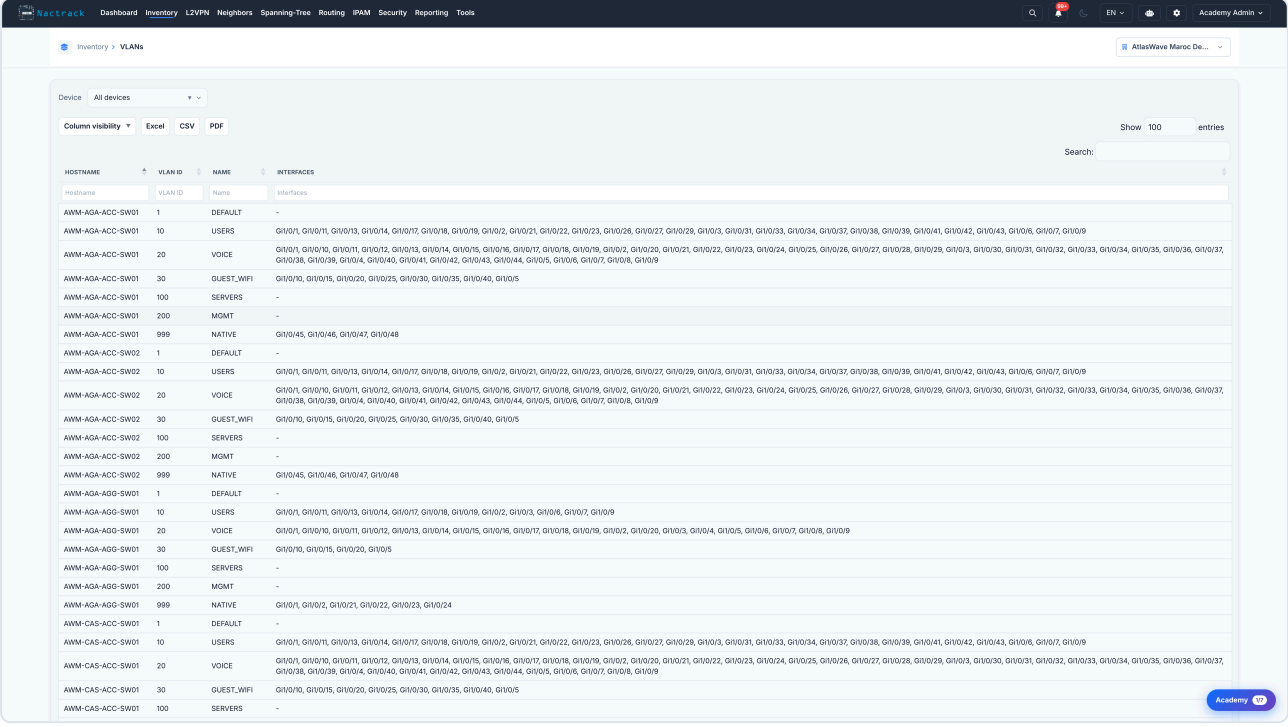
- 1 Ouvrez Inventory puis VLANs. Chaque ligne correspond à un VLAN sur un switch, qui est précisément le niveau auquel la question doit être posée.



The screenshot shows the Nectrack web interface with the 'Inventory' tab selected and 'VLANs' viewed. The table lists VLANs for various switches, including AWM-AGA-ACC-SW01, AWM-AGA-ACC-SW02, AWM-AGA-ACC-SW03, AWM-AGA-ACC-SW04, AWM-AGA-ACC-SW05, AWM-AGA-ACC-SW06, AWM-AGA-ACC-SW07, AWM-AGA-ACC-SW08, AWM-AGA-ACC-SW09, AWM-AGA-ACC-SW10, AWM-AGA-ACC-SW11, AWM-AGA-ACC-SW12, AWM-AGA-ACC-SW13, AWM-AGA-ACC-SW14, AWM-AGA-ACC-SW15, AWM-AGA-ACC-SW16, AWM-AGA-ACC-SW17, AWM-AGA-ACC-SW18, AWM-AGA-ACC-SW19, AWM-AGA-ACC-SW20, AWM-AGA-ACC-SW21, AWM-AGA-ACC-SW22, AWM-AGA-ACC-SW23, AWM-AGA-ACC-SW24, AWM-AGA-ACC-SW25, AWM-AGA-ACC-SW26, AWM-AGA-ACC-SW27, AWM-AGA-ACC-SW28, AWM-AGA-ACC-SW29, AWM-AGA-ACC-SW30, AWM-AGA-ACC-SW31, AWM-AGA-ACC-SW32, AWM-AGA-ACC-SW33, AWM-AGA-ACC-SW34, AWM-AGA-ACC-SW35, AWM-AGA-ACC-SW36, AWM-AGA-ACC-SW37, AWM-AGA-ACC-SW38, AWM-AGA-ACC-SW39, AWM-AGA-ACC-SW40, AWM-AGA-ACC-SW41, AWM-AGA-ACC-SW42, AWM-AGA-ACC-SW43, AWM-AGA-ACC-SW44, AWM-AGA-ACC-SW45, AWM-AGA-ACC-SW46, AWM-AGA-ACC-SW47, AWM-AGA-ACC-SW48, AWM-AGA-ACC-SW49, AWM-AGA-ACC-SW50, AWM-AGA-ACC-SW51, AWM-AGA-ACC-SW52, AWM-AGA-ACC-SW53, AWM-AGA-ACC-SW54, AWM-AGA-ACC-SW55, AWM-AGA-ACC-SW56, AWM-AGA-ACC-SW57, AWM-AGA-ACC-SW58, AWM-AGA-ACC-SW59, AWM-AGA-ACC-SW60, AWM-AGA-ACC-SW61, AWM-AGA-ACC-SW62, AWM-AGA-ACC-SW63, AWM-AGA-ACC-SW64, AWM-AGA-ACC-SW65, AWM-AGA-ACC-SW66, AWM-AGA-ACC-SW67, AWM-AGA-ACC-SW68, AWM-AGA-ACC-SW69, AWM-AGA-ACC-SW70, AWM-AGA-ACC-SW71, AWM-AGA-ACC-SW72, AWM-AGA-ACC-SW73, AWM-AGA-ACC-SW74, AWM-AGA-ACC-SW75, AWM-AGA-ACC-SW76, AWM-AGA-ACC-SW77, AWM-AGA-ACC-SW78, AWM-AGA-ACC-SW79, AWM-AGA-ACC-SW80, AWM-AGA-ACC-SW81, AWM-AGA-ACC-SW82, AWM-AGA-ACC-SW83, AWM-AGA-ACC-SW84, AWM-AGA-ACC-SW85, AWM-AGA-ACC-SW86, AWM-AGA-ACC-SW87, AWM-AGA-ACC-SW88, AWM-AGA-ACC-SW89, AWM-AGA-ACC-SW90, AWM-AGA-ACC-SW91, AWM-AGA-ACC-SW92, AWM-AGA-ACC-SW93, AWM-AGA-ACC-SW94, AWM-AGA-ACC-SW95, AWM-AGA-ACC-SW96, AWM-AGA-ACC-SW97, AWM-AGA-ACC-SW98, AWM-AGA-ACC-SW99, AWM-AGA-ACC-SW100.

HOSTNAME	VLAN ID	NAME	INTERFACES
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/47, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/47, G1/0/9
AWM-AGA-ACC-SW02	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW02	100	SERVERS	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW03	1	DEFAULT	-
AWM-AGA-ACC-SW03	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/47, G1/0/9
AWM-AGA-ACC-SW03	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW03	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW03	100	SERVERS	-
AWM-AGA-ACC-SW03	200	MGMT	-
AWM-AGA-ACC-SW03	999	NATIVE	G1/0/1, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/24
AWM-CAS-ACC-SW01	1	DEFAULT	-
AWM-CAS-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/47, G1/0/9
AWM-CAS-ACC-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-CAS-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-CAS-ACC-SW01	100	SERVERS	-

- 2 Parcourez la colonne Interfaces. Un tiret signifie que le VLAN est défini sur ce switch mais qu'aucun port d'accès, de voix ou natif ne lui est affecté. Sur ce switch d'accès, les VLAN utilisateurs et voix sont peuplés alors que ceux des serveurs et du management ne le sont pas, ce qui est attendu en périphérie.



The screenshot shows the 'Inventory > VLANs' page in the NACStack interface. The table displays VLAN configurations for various switches, including their names, VLAN IDs, names, and the interfaces they are connected to. The 'Interfaces' column contains lists of interface names, with dashes indicating no interfaces are connected.

HOSTNAME	VLAN ID	NAME	INTERFACES
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/9, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/9, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-ACC-SW02	20	VOICE	G1/0/1, G1/0/9, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	G1/0/9, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW02	100	SERVERS	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-AGG-SW01	1	DEFAULT	-
AWM-AGA-AGG-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/3, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-AGG-SW01	20	VOICE	G1/0/1, G1/0/9, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/3, G1/0/4, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-AGG-SW01	30	GUEST_WIFI	G1/0/9, G1/0/15, G1/0/20, G1/0/5
AWM-AGA-AGG-SW01	100	SERVERS	-
AWM-AGA-AGG-SW01	200	MGMT	-
AWM-AGA-AGG-SW01	999	NATIVE	G1/0/1, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/24
AWM-CAS-ACC-SW01	1	DEFAULT	-
AWM-CAS-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/6, G1/0/7, G1/0/9
AWM-CAS-ACC-SW01	20	VOICE	G1/0/1, G1/0/9, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-CAS-ACC-SW01	30	GUEST_WIFI	G1/0/9, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-CAS-ACC-SW01	100	SERVERS	-

BON À SAVOIR

Un tiret ne signifie pas que le VLAN est inutilisé. Il signifie qu'aucun port d'ACCÈS de ce switch n'y est rattaché. Le VLAN peut malgré tout être transporté par les trunks du switch pour d'autres équipements, et le supprimer les casserait.

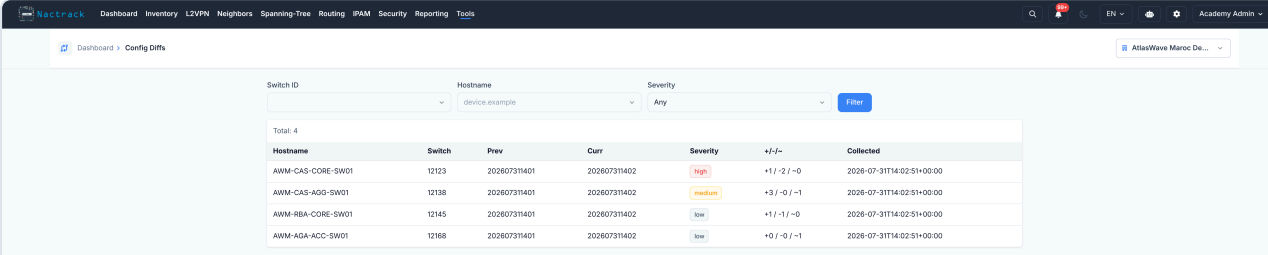
Il n'existe pas de rapport "VLAN inutilisés" à l'échelle du parc, ni de filtre sur les VLAN vides. Il s'agit de la lecture d'une liste, switch par switch, ce qui explique son classement dans le niveau compréhension plutôt que recherche.

Comment savoir ce qui a changé sur le réseau entre deux collectes

La plupart des pannes suivent un changement, et le plus difficile est rarement le correctif. C'est d'établir ce qui a bougé et sur quel équipement, à un moment où personne ne se déclare volontaire pour avoir touché à quoi que ce soit. NacTrack compare la configuration de chaque équipement à sa collecte précédente et enregistre ce qui a été ajouté, supprimé et modifié : la question n'est plus qui a changé quelque chose, mais lequel de ces changements peut produire le symptôme.

Nécessite: module: core, permission: use_troubleshooting, vendors: All collected platforms; the comparison is on configuration text

- 1 Le suivi des changements se trouve avec les outils de dépannage plutôt qu'avec l'inventaire, car on y recourt lorsqu'on a déjà un symptôme en main.
- 2 Chaque ligne correspond à un équipement dont la configuration diffère de la collecte précédente. Prev et Curr identifient les deux collectes comparées, et les trois compteurs indiquent les lignes ajoutées, supprimées et modifiées. Un changement comportant des suppressions mérite plus d'attention qu'un ajout seul : supprimer une ligne, c'est ainsi que quelque chose cesse de fonctionner.

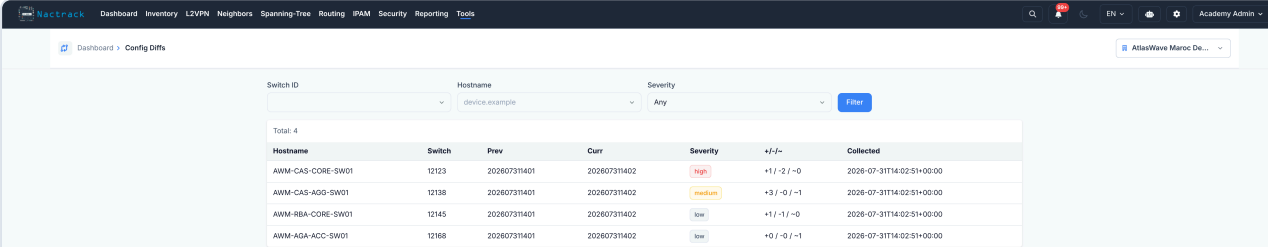


Switch ID: Hostname: Severity:

Total: 4

Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00
AWM-CAS-AGG-SW01	12138	202607311401	202607311402	Medium	+3 / -0 / -1	2026-07-31T14:02:51+00:00
AWM-RBA-CORE-SW01	12145	202607311401	202607311402	Low	+1 / -1 / -0	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	12168	202607311401	202607311402	Low	+0 / -0 / -1	2026-07-31T14:02:51+00:00

- 3 La gravité traduit l'appréciation de NacTrack sur ce qui a été touché, non sur le nombre de lignes déplacées. La ligne de gravité haute a ici supprimé deux lignes et en a ajouté une, tandis qu'une ligne de gravité basse plus bas n'a modifié qu'une ligne. Moins de lignes, plus de conséquences.

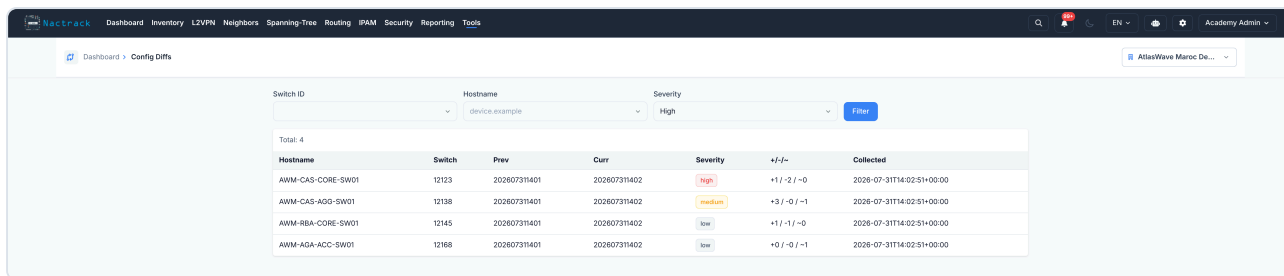


Switch ID: Hostname: Severity:

Total: 4

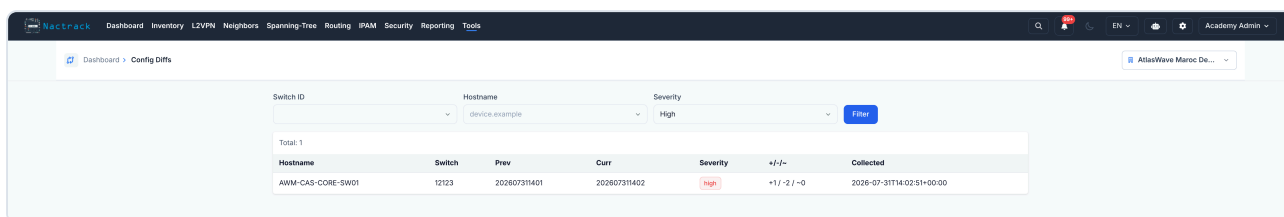
Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00
AWM-CAS-AGG-SW01	12138	202607311401	202607311402	Medium	+3 / -0 / -1	2026-07-31T14:02:51+00:00
AWM-RBA-CORE-SW01	12145	202607311401	202607311402	Low	+1 / -1 / -0	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	12168	202607311401	202607311402	Low	+0 / -0 / -1	2026-07-31T14:02:51+00:00

- 4 Avec un symptôme et une fenêtre de temps, filtrez sur la gravité à lire en premier. Sur un parc réel, cette liste compte des centaines de lignes par semaine : commencer par les gravités hautes est ce qui en fait un diagnostic plutôt qu'une lecture.



Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00
AWM-CAS-AGG-SW01	12138	202607311401	202607311402	Medium	+3 / -0 / -1	2026-07-31T14:02:51+00:00
AWM-RBA-CORE-SW01	12145	202607311401	202607311402	Low	+1 / -1 / -0	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	12168	202607311401	202607311402	Low	+0 / -0 / -1	2026-07-31T14:02:51+00:00

- 5 Un seul équipement reste. C'est le candidat : un commutateur de coeur ayant perdu deux lignes de configuration entre deux collectes le même jour. À partir de là, la page de l'équipement donne ses voisins, ses interfaces et son état de conformité : c'est là que le diagnostic se poursuit.



Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00

BON À SAVOIR

Ceci compare des collectes, pas des instants. Deux modifications effectuées entre les deux mêmes collectes apparaissent comme une seule différence combinée, et une modification faite puis annulée avant la collecte suivante ne laisse aucune trace.

Un changement listé ici ne prouve pas la panne, et son absence ne prouve pas l'innocence. Beaucoup de pannes proviennent de quelque chose d'entièrement extérieur à la configuration : un optique défaillant, le changement d'un voisin, un certificat expiré.

La gravité est attribuée selon le type de configuration modifiée : elle reflète donc la portée et non l'intention. Un changement volontaire et validé sur une instruction de routage reste classé en gravité haute.