

PingCastle

Qu'est ce que Pingcastle ?

Pingcastle est un outil de sécurité (comme lynis pour linux) qui évalue le niveau de sécurité d'un environnement Windows Server.

Pratique

Tout d'abord, il faut installer PingCastle sur le Windows Server, extraire le dossier téléchargé. Ensuite on peut procéder de 2 façons, soit on décide de directement lancer le "PingCastle.exe" depuis le dossier PingCastle

① Active_Directory_Security_Self_Assessme...	24/01/2025 10:43	Opera GX Web Do...	2 739 Ko
📄 changelog	24/01/2025 10:43	Document texte	37 Ko
📄 license	24/01/2025 10:43	Document au for...	13 Ko
① PingCastle v3.0.0	24/01/2025 10:43	Opera GX Web Do...	1 657 Ko
PingCastle	24/01/2025 10:43	Application	2 678 Ko
📄 PingCastle.exe.config	24/01/2025 10:43	Fichier CONFIG	6 Ko
🚀 PingCastleAutoUpdater	24/01/2025 10:43	Application	89 Ko
📄 PingCastleAutoUpdater.exe.config	24/01/2025 10:43	Fichier CONFIG	1 Ko

Soit on se rend sur l'invite de commande du PC (CMD), on rentre le chemin d'accès du dossier et on tape la commande "PingCastle.exe".

```
C:\Users\Administrator>C:\Users\Administrator\Desktop\PingCastle.exe
```

Dans les 2 cas, cela lancera PingCastle. On peut ensuite choisir ce qu'on veut faire, vérifier, etc....

```
\---o---  PingCastle (Version 3.3.0.1  25/09/2024 21:03:40)
 \ / \ ``-> Get Active Directory Security at 80% in 20% of the time
 0---o   End of support: 2026-01-31
  \ ,` For find out more about PingCastle, visit https://www.pingcastle.com
   v  For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
    For support and questions:
     - Open-source community, visit https://github.com/netwrix/pingcastle/issues
     - Customers, visit https://www.netwrix.com/support.html

What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
 1-healthcheck-Score the risk of a domain
 2-azuread  -Score the risk of AzureAD
 3-conso   -Aggregate multiple reports into a single one
 4-carto   -Build a map of all interconnected domains
 5-scanner  -Perform specific security checks on workstations
 6-export   -Export users or computers
 7-advanced -Open the advanced menu
 0-Exit

=====
This is the main functionality of PingCastle. In a matter of minutes, it produces a report which will give you an overview of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

A la fin des analyses, PingCastle fera un rapport sous forme de fichier à ouvrir sur un navigateur de recherche. Ce rapport, affiche une jauge correspondant au niveau de sécurité de l'infrastructure et se trouve dans le dossier PingCastle. Ce rapport donne aussi des astuces/conseilles pour améliorer la sécurité du Windows Server.

winsrv.fr 2025-01-24 About

winsrv.fr - Healthcheck analysis

Date: 2025-01-24 - Engine version: 3.3.0.1

This report has been generated with the Basic Edition of PingCastle [?](#).
Being part of a commercial package is forbidden (selling the information contained in the report).
If you are an auditor, you MUST purchase an Auditor license to share the development effort.

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

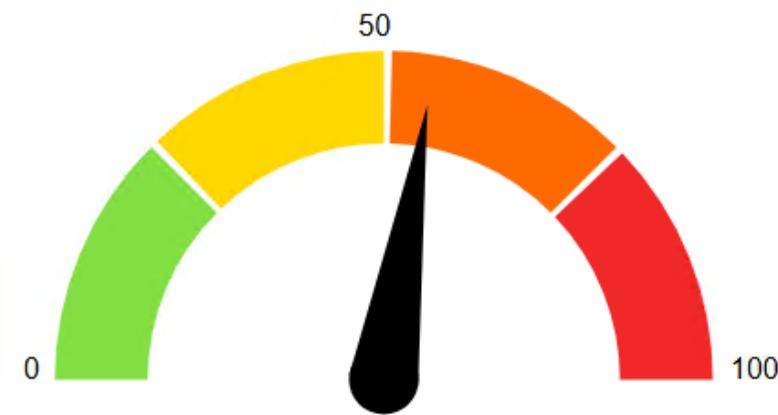
Domain Risk Level: 55 / 100
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better
[Compare with statistics](#)
[Privacy notice](#)

Stale Object : 31 / 100
It is about connections related to objects
10 rules matched

Trusts : 0 / 100
It is about connections between trust Active
0 rules matched

winsrv.fr Consolidation 2025-01-24 About

Average Risk Level: 55 / 100
Best Risk Level: 55 / 100
Worst Risk Level: 55 / 100
Median Risk Level: 55 / 100



Risk model [?](#)

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential