

A backup copy that a server can write to is not separate from that server

About 30 minutes, on one server, with no new tools

A U.S. ransomware guide from CISA, the FBI and the NSA says actors "attempt to find and subsequently delete or encrypt accessible backups". This page shows what accessible means for one server.

Yes 2 Written down, with a date (a log, a screen, a document), and it meets your own plan.

Partly 1 Remembered, but not written down, or the record shows you missed your plan.

No 0 Nobody knows, or it was never done. A blank is a finding.

"None, checked on a date" counts as a record. No plan or target written down? Write your guess first, then measure: the guess is your plan.

Five questions about your own setup

1 Routes from one server

Your answer, and where it is written down (with the date) Pick the everyday server your staff use most. Signed in the way an administrator normally does, what routes to the backup copy does it show? Write the server, the date, and each route, or none found.

No 0 | Partly 1 | Yes 2 | Score 0, 1 or 2 | This quarter | Next quarter

How to raise it

Where to find it:
On Windows, open This PC in File Explorer for mapped drives (a lettered drive that points to another machine). On Linux, list the mounted shares (folders on another machine that appear as local folders). Write one line per route, or write none found with today's date.

To get it to a 2:
A dated note for that server listing every route, or none found. No plan written down for what this server may reach? Write your guess (for example, nothing) and score against it.

What this does not prove:
One server is not every server. A route can also exist that this sign-in cannot see.

A sheet to fill in, one line per account that reaches a copy: who can delete your backups, place by place

2 Did a route accept a write

Your answer, and where it is written down (with the date) For each route you found, did it accept an empty text file named with today's date? Write yes or no beside each route.

No 0 | Partly 1 | Yes 2 | Score 0, 1 or 2 | This quarter | Next quarter

How to raise it

Where to find it:
Save the empty file to the route, note whether it was accepted, and delete only that file. Write the answer and the date next to the route's line. No route found: write none found, checked and the date.

To get it to a 2:
A dated yes or no for every route, and no yes left open. A yes that was closed and tested again, with both dates written, counts.

What this does not prove:
A no today shows this route refused one file today. It does not show the route stays closed after the next change.

3 Saved sign-ins to the backup system

Your answer, and where it is written down (with the date) Does the server hold a saved sign-in to the backup system, even when no drive is mapped? Write where you looked and the date.

No 0 | Partly 1 | Yes 2 | Score 0, 1 or 2 | This quarter | Next quarter

How to raise it

Where to find it:
On Windows, open Credential Manager (the list of sign-ins the server has saved) and look for any entry that names the backup system. Write each one down, or write none found with the date.

To get it to a 2:
A dated list of every saved sign-in to the backup system found, or none found, checked on a date. Each one on the list has a decision beside it: keep or remove, with a name.

What this does not prove:
This check does not test the backup software's own accounts, which are a separate list.

4 Servers with a dated answer

Your answer, and where it is written down (with the date) How many of the servers that hold the most data have a dated yes or no for rows 1 to 3? Write that count next to the count of servers on your list.

No 0 | Partly 1 | Yes 2 | Score 0, 1 or 2 | This quarter | Next quarter

How to raise it

Where to find it:
Your server list or asset list for the servers, and the dated notes from rows 1 to 3 for the answers. No list? Write the five servers your staff would miss first.

To get it to a 2:
Every server on the list has a dated answer for rows 1 to 3, inside the interval your plan sets. No interval written down? Write your guess (once a year, once a quarter) and score against it.

What this does not prove:
Your list shows which servers you chose to check. It does not show the ones you left off.

5 What happens next

Your answer, and where it is written down (with the date) If any route accepted the test file, who is closing it, and by what date? If none did, when is the next check?

No 0 | Partly 1 | Yes 2 | Score 0, 1 or 2 | This quarter | Next quarter

How to raise it

Where to find it:
Your change ticket or team calendar, with a named person and a date.

To get it to a 2:
A named person and a date on the ticket or calendar, inside your plan's interval. If a route is still open, the closing date is written and the ticket exists.

Your total, out of 10

9-10 **Known** Score the same page again next quarter.

5-8 **Partly known** Fix your lowest row this week.

0-4 **Assumed** Do row 1 this week.

Two rules beat the total: if row 1 scores below 2, the result is Assumed. Any row that missed your plan or guess is your next step.

> From your busiest file server, could you open the backup copy like a folder?

What this does not prove

A dated no for one server shows that server could not write to the backup copy that day. It does not show every server is out of reach, or that the backup software's own accounts are safe.

Made by StepKnock, a small team in San Diego, paid through our partners when a customer buys. This page sells nothing.

Nothing to sign up for. No cookies, no analytics, and nothing you type here leaves this page.

stepknock.com/toolkit/checks/server-reach-to-backup/