ScriptPreflight

Preflight report

Synthetic sample. Not a customer script.

Script
restart-servers.ps1

Report ID
00000000-0000-4000-8000-00000000a002

Date
6 November 2026, 22:54 SAST (20:54 UTC)

Version
Engine 0.1.0 · ruleset 0.6.2

Result

High risk · Do not run as written

It restarts every computer in the domain, not the 3 you meant.

What it changes

Restarts computers, with -Force.

`Restart-Computer · line 5`

How far it reaches

Every computer account Get-ADComputer returns. The count can't be known from the script alone.

`Every computer account returned by Get-ADComputer (count unknown without environment context) (Restart-Computer)`

Can you undo it

Partly. Computers come back; open sessions and unsaved work are lost.

`reversibility: conditional`

What you meant, and what it can reach

You said — **3 computers**

It can reach — **every computer account · count unknown**

What we could check: partly

- Required roles and permissions are not assessed for Get-ADComputer (no permission catalogue yet for Active Directory).
- Commands run on remote computers whose state and identity are not known.

Also note

- Synthetic sample, not a real customer script. Findings, blast radius, coverage and the rewrite re-check are real engine output; the explanation, rewrite and plans were written by our team to illustrate the AI explainer, which is not switched on yet.
- PSScriptAnalyzer baseline is not yet enabled in engine 0.1; only ScriptPreflight rules ran.
- No live tenant or server data was used: object counts are not known.

Findings (4)

Most severe first: 2 high, 1 medium, 1 low.

High Unfiltered tenant-wide target

SPF-MG-014 · version 0.4.1 · line 5

```
5 Get-ADComputer -Filter * | ForEach-Object { Restart-Computer -ComputerName $_.Name -Force }
```

Why it matters

Get-ADComputer -Filter * returns every computer object, and each one is passed to Restart-Computer.

Recommendation

Limit Get-ADComputer to the intended computers with -Filter or -SearchBase (for example one OU in the maintenance window), export the list for review, and act on it in batches.

High Every discovered computer restarted or shut down

SPF-WIN-001 · version 0.6.2 · line 5

```
5 Get-ADComputer -Filter * | ForEach-Object { Restart-Computer -ComputerName $_.Name -Force }
```

Why it matters

-Force restarts machines even when users are signed in, so open work is lost on every affected computer.

Recommendation

Do not feed an unfiltered Get-ADComputer into Restart-Computer: limit it with -Filter or -SearchBase to the intended servers, export and review the list, then restart in batches inside a maintenance window and check each server is back before continuing.

Medium State changes have no error handling

SPF-CORE-021 · version 0.3.0 · line 5

```
5 Get-ADComputer -Filter * | ForEach-Object { Restart-Computer -ComputerName $_.Name -Force }
```

Why it matters

1 state-changing command(s) (Restart-Computer) continue after errors, which can leave a partial change with no record.

Recommendation

Add -ErrorAction Stop and wrap the change in try/catch that records what completed.

Low Console-only output

SPF-CORE-040 · version 0.3.0 · line 7

```
7 Write-Host "Restart requested"
```

Why it matters

Write-Host leaves no audit trail of what was changed.

Recommendation

Use Start-Transcript or write a log file recording each object changed.

Suggested fix

Before

```
1 - # SYNTHETIC SAMPLE: restart the web servers after patching
2 - # Intended: restart WEB01, WEB02 and WEB03 only
3 - Import-Module ActiveDirectory
4 -
5 - Get-ADComputer -Filter * | ForEach-Object { Restart-Computer -ComputerName $_.Name -Force }
6 -
7 - Write-Host "Restart requested"
```

After

```
1 + #Requires -Modules ActiveDirectory
2 + param([switch]$Apply)
3 + $targets = @('WEB01', 'WEB02', 'WEB03')
4 + $computers = foreach ($name in $targets) { Get-ADComputer -Identity $name -ErrorAction Stop }
5 + $computers | Select-Object Name, DNSHostName | Export-Csv -Path 'C:\Change\restart-targets.csv'
        -NoTypeInformation
6 + foreach ($c in $computers) {
7 +     if ($Apply) {
8 +         Restart-Computer -ComputerName $c.DNSHostName -Confirm -ErrorAction Stop
9 +     } else {
10 +         Restart-Computer -ComputerName $c.DNSHostName -WhatIf
11 +     }
12 + }
```

Checked again by the same engine: the fix parses and clears 3 of 4 rules found. Still flagged: remote computers restarted or shut down (medium, line 8 of the fix).

Illustrative rewrite written by our team: explicit WEB01-03 list, -WhatIf by default, -Confirm on apply, pre-change export, stop on errors.

Pilot, verify, roll back

Pilot

1. Run the rewrite without -Apply and review the -WhatIf output: it must list WEB01, WEB02 and WEB03 only.
2. Apply to WEB01 first and confirm it returns to service before continuing.

Verify

1. Check each server is reachable and its web service responds.
2. Compare restart-targets.csv with the change ticket.

Roll back

1. A restart cannot be undone. If a server does not come back, follow the server recovery runbook and stop the change.

Point of no return: The first Restart-Computer call with -Apply.

Sign-off

Reviewed by _____

Approved by _____

Change ref _____

Date _____