PH7X SYSTEMS ®

0.1.0 · CHAPTER 38

Switch off the old farm in an order you can stop at every step but the last

SharePoint Migration Field Guide · Chapter 38

pH7x Systems

2026-11-07

38. Switch off the old farm in an order you can stop at every step but the last

> A farm outlives its servers in every system that was told to trust it.

Chapter 9 set the evidence gate for decommissioning each wave's source, and Chapter 27 gave every archive that outlives the farm a home elsewhere. This chapter starts when both hold for the whole farm, and switches off what remains: its servers, its databases and everything outside SharePoint that still expects it to answer, whether the content went to Subscription Edition by attach (Chapter 23) or to SharePoint Online by copy (Chapter 8).

> **What is switched off, in what order, and what stays documented once the farm is gone?**

The decision this chapter leads to is the decommissioning sequence: each step with its owner, its reversal while that still exists, and the evidence kept, read backwards from the Chapter 2 inventory.

Which farms this chapter is for

Every SharePoint Server 2016 or 2019 farm whose content has gone, including those nobody administers. After an attach, the fallback Microsoft documents is the original farm, so switching it off ends rollback: start after the expiry date Chapter 9 wrote. After a copy, the source has been read-only since cutover. A farm running hybrid leaves it first, by Chapter 25's sequence; one publishing a service application waits until its consumers have moved off it (Chapter 10).

”Just in case” needs a case

At the end of support, a product gets "no new security updates, non-security updates, free or paid assisted support options or online technical content updates"; SharePoint Server 2016 and 2019 reached it on 14 July 2026, as did SQL Server 2016 (ending support in 2026, checked on 7 November 2026).

A farm kept running just in case is kept for a case nobody wrote down. Three already have a home: a rollback has Chapter 9's expiry date, an obligation on content a Chapter 27 row, and a question about what the farm held the record and final backups below. We would have the farm's owner write down any other case, with an end date, or start the sequence.

The gate, the holds and the silence

The sequence starts when every wave has passed Chapter 9's gate, every Chapter 26 deletion has its row, Chapter 14's exports are archived and no Chapter 27 row still needs the farm. A farm refuses to delete a site collection on hold, as Chapter 26 found, but SQL Server drops a database without asking the farm: no source in its eDiscovery Center may still be on hold, and only the case owner releases one (Chapter 27).

Then listen: read every front end's IIS logs with Chapter 22's method, over a window that includes a month end. Each account or address still calling is an integration nobody re-pointed or a person nobody told; we would keep counts, not names (Chapter 14). What reads the databases directly never reaches those logs; step 6 finds it.

The sequence

Microsoft documents the parts, but no page we found retires a whole farm, so this order is ours: reversible steps first, while the farm is whole; then a quiet period with it stopped; no deletion until the final backups are proven. Each step's owner performs it and signs its evidence.

STEP	WHERE IT LIVES, AND WHO OWNS IT	HOW IT IS REMOVED	REVERSIBLE UNTIL	EVIDENCE KEPT
1. Names that send people to the farm	DNS, load balancers; the network team	Re-pointed to the destination, or to a redirect with an owner and an end date	Until step 8: restore the record	Records before and after
2. Trusts others hold for the farm	AD FS, other farms, the tenant; their owners	Relying party disabled, then removed; trust deleted on the other farm; Chapter 25's exit	Disabled: enabled again. Deleted: recreated from the exports	Trusts and certificates, exported
3. Services bound to the farm	Office Online Server, Workflow Manager; their administrators	`Remove-SPWOPIBinding`; the farm's domain off the allow list; each workflow node leaves its farm	Binding recreated; node rejoined with the Certificate Generation Key	Bindings, allow list, key, scope
4. The farm's servers, tasks and monitors	Servers, schedulers, monitoring; the farm administrators	Shut down; tasks disabled; monitors paused for a quiet period	Restarted, while its accounts are enabled and their passwords agree	What failed or complained meanwhile
5. Final backups	SQL Server; the database administrators	Full, with checksums, each restored elsewhere and checked	Nothing: later steps rely on them	Checksums, restore tests, keys' location, end date
6. The farm's databases	SQL Server; the database administrators	Detached	Attached again	What was detached, and where the files are
7. Accounts, service principal names (SPNs), certificates, server records, firewall rules, jobs, monitors	Active Directory, the certificate authority, DNS, firewalls, tools; their owners	Disabled, then deleted; `setspn -D`; certificates revoked or left to expire	Deleted accounts: only through an Active Directory Recycle Bin enabled beforehand	Each list before removal
8. Last: database files, server disks	Storage, servers; the infrastructure owner	Deleted; disks wiped under the media policy	Never: only the final backups remain	Who, what, when

Steps 1 to 4: cut what points at the farm, then stop it

The farm's alternate access mappings, and `Get-SPSiteUrl` for host-named site collections (host-named sites), list the names for step 1. A disabled relying party trust means AD FS "does not issue tokens" for it (Disable-AdfsRelyingPartyTrust). Farms that share service applications hold each other's root certificates, and the publishing farm the consumer's STS certificate too (exchange trust certificates); each copy stays until the other farm's Manage trust page deletes it.

`New-SPWOPIBinding` recreates what `Remove-SPWOPIBinding` removes (Remove-SPWOPIBinding). An empty Office Online Server allow list "allows file requests to hosts in any domain" (Remove-OfficeWebAppsHost): remove the old farm's domain only while another host's stays, or retire that farm too. A Workflow Manager node leaves through its configuration wizard and cannot rejoin "without a valid Certificate Generation Key" (install and configure workflow); after an attach, nodes that rejoined after Chapter 19's backup leave again.

Microsoft's guidance schedules farm backups as scripts in Windows Task Scheduler (backup best practices), so look for such tasks beyond the farm's own servers, and disable them with it. The quiet period is your convention; we would include a month end. A restart needs the passwords to agree: when Active Directory and the farm disagree, "services in the SharePoint farm won't start" (automatic password change), which is why accounts wait for step 7. All checked on 7 November 2026.

Steps 5 and 6: a backup that something can still open

Take full backups: "detaching a read-only database loses information about the differential bases of differential backups", while the detached files stay "intact" (detach and attach). Prove them: "You don't have a restore strategy until you test your backups", which means a restore on a test system and `DBCC CHECKDB` (back up and restore).

We found no period for which Microsoft says a backup stays restorable, only version rules. A farm backup made with SharePoint's tools cannot restore to another version or "upgrade to another version", so it needs the 2016 or 2019 farm being retired, and neither SharePoint's tools nor SQL Server's back up a transparent data encryption key (prepare to back up and restore). A SQL Server backup restores on its own version or a later one, never an earlier one (RESTORE), and Subscription Edition attaches 2016 and 2019 databases at version 16.0.4351.1000 or higher (upgrade overview); for how long it will, we do not know. We would prove one final content database on a test Subscription Edition farm, or record its readability as not established.

Record where the keys are, never the keys: that encryption key, Secure Store's pass phrase (Chapter 10) and Workflow Manager's Certificate Generation Key (Chapter 19). After a copy, the backups also hold the audit entries Chapter 14 found no Microsoft tool to carry online. Their end date comes from the obligation behind them, set by its owner (Chapter 6); content somebody must read belongs in Chapter 27's archive, not a backup nobody can search. **A final backup is evidence only while something can still open it.**

Detach only databases on the old farm's own list, read before it stopped and checked against the new farm's: on a shared SQL Server, a name is not an owner. Whatever still reads them directly fails now, and attaching undoes it. All checked on 7 November 2026.

Steps 7 and 8: what Microsoft's removal pages cover

Microsoft's page removes a server from a farm that carries on: `Disconnect-SPConfigurationDatabase`, the method it recommends, "only removes the local SharePoint server", and without the server running Central Administration you are "unable to administer the server farm" (remove a server). Uninstalling leaves "Web.config files, index files, log files" and customisations, and "all user data remains in the database files" (uninstall). Deleting a service application "is permanent", its database optional, after a backup Microsoft suggests (delete a service application). On a farm that ends we would do none of it piece by piece: databases leave at steps 6 and 8, disks are wiped, and only a server being reused is uninstalled, Central Administration's last.

The farm registered accounts that already existed; its registration page has "no options" to create one (managed accounts). Disable each only after checking that no other system, the new farm first, uses it; delete it later. The Recycle Bin "isn't enabled by default" and restores only deletions made after it was (Recycle Bin). `setspn -L` lists an account's SPNs, `-Q` finds who holds one, `-X` finds duplicates (setspn); an SPN for a name the new farm answers on stays on its account. Firewall rules follow the ports Microsoft lists for a farm, from SQL Server's 1433 to the service applications' 32843 to 32845 (security hardening). All checked on 7 November 2026.

What stays documented, and where

Read Chapter 2's inventory backwards and each line closes here: each farm gets a sequence; content databases end at steps 5, 6 and 8; customisations and authentication in the configuration below and at steps 2 and 7; integrations in the silent window; workflows at step 3; usage in Chapter 14's exports; constraints in the backups' end date.

The decommissioning record holds each step's owner, date, reversal and result; the silent window's counts; the backups' checksums, restore tests, keys' location and end date; and the farm's configuration as last read, before step 4: servers, databases, service applications, managed accounts, trusts, bindings, solutions and alternate access mappings. Store it with Chapter 9's verification records and the sign-off papers, somewhere that outlives the project and no step removes, with its own owner and an end date, the latest of the obligations it serves. **The farm is gone when its record closes, not when its servers stop.**

Out of scope

Verification and the gate are Chapters 8 and 9, archives Chapter 27, leaving hybrid Chapter 25, repointing integrations Chapter 22, keeping a Subscription Edition farm current Chapter 42, and measuring what the project achieved Chapter 40. Secure destruction of physical media, backup and retention design, contracts, licences and costs are not covered.

Before you continue

- [ ] Every wave passed Chapter 9's gate, its rollback date has passed, and no Chapter 27 row needs the farm
- [ ] Nothing on the farm is on hold, and its front ends were silent over a window that included a month end
- [ ] Every step has an owner, a written reversal while one exists, and its evidence
- [ ] Names, trusts and bindings were re-pointed or disabled before the servers stopped
- [ ] The final backups are full, checksummed and restored once, with their keys' location and an end date from an obligation's owner
- [ ] Only the old farm's own databases were detached, and nothing was deleted before the quiet period ended and the backups were proven
- [ ] Every account, SPN, certificate, record, rule, job and monitor was listed before removal, and none serves another system
- [ ] The record, with the configuration as last read, sits with Chapter 9's records, with its own owner and end date