

PH7X SYSTEMS ®

1.0.0 · CHAPTER 7

Run hybrid as a farm you patch, watch by hand and test on a schedule, with a rehearsed way back

Hybrid Architecture Field Guide · Chapter 7

pH7x Systems

2026-11-13

7. Run hybrid as a farm you patch, watch by hand and test on a schedule, with a rehearsed way back

> Microsoft 365 updates itself. The farm, the trust and the synchronisation that connect to it are yours, and nothing in the product tells you when one of them stops.

A hybrid farm stays a farm. Microsoft 365 installs none of its updates, renews none of its certificates and watches none of its timer jobs. Microsoft documents how to configure each hybrid feature and how to remove it. On running one, the pages we read are silent: no health rule, monitoring guidance or diagnostic category is specific to the redirects, to taxonomy replication or to the trust.

> **Who keeps this hybrid farm supported and connected, with which checks, how often, and what do they do when a check fails?**

The decision this chapter leads to is an operating model: a patch rhythm, a list of checks with an owner and a frequency for each, a first check for each failure, and a recovery that was rehearsed before it was needed.

What this chapter settles

It settles what the team owns while any hybrid feature runs, and how it shows that hybrid still works. It takes the feature list and the supported build from Chapter 1, the trust, its read-only script and the Certificate Register from Chapter 2, each feature's checks from Chapters 3, 4 and 5, and the governance control matrix from Chapter 6. It hands the order of removal to Chapter 8.

It leaves out how to install a public update, which is Chapter 42 of the SharePoint Migration Field Guide and the analysis on updating without downtime, and the design of the farm's backups.

Applies to

FACT	SHAREPOINT SERVER 2016 AND 2019	SUBSCRIPTION EDITION
Servicing	Ended on 14 July 2026 (Chapter 1)	Each public update build is supported for one year
End-of-support notices for the installed build	No	From Version 24H2
Zero downtime patching	Documented	Documented; needs a highly available farm
Feature release rings	No	From Version 22H2; cmdlets from Version 23H2
Certificate health analyzer rules	No	Four rules, for SSL certificates

Architecture

Everything that remains of hybrid runs outbound from the farm (Chapter 1), so every moving part is on your side or in your directory.

PART	WHAT KEEPS IT WORKING	WHAT MICROSOFT SAYS
The farm's build	You install each public update	"To remain supported, you must be running a supported build"
The trust: realm, trusted token issuer, proxies, the tenant's principal	Nothing changes it unless somebody does	The realm "must always match the tenant context identifier. If you change this value, the farm will no longer participate in hybrid functionality."
The STS signing certificate	Nothing, while it is the default; a replacement expires	"The default STS certificate does not need to be renewed."
Directory synchronisation	The identity team keeps the tool supported	"synchronization services will stop working after this date if these requirements aren't met"
Service applications	Managed Metadata, User Profile, My Sites, App Management and Subscription Settings, on the local farm	Chapter 2
Each feature	A crawl, a timer job or a setting	Below

Sources: Subscription Edition servicing policy, configure server-to-server authentication, replace the STS certificate and Entra Connect version history, all checked on 13 November 2026.

One dependency shapes diagnosis. Server-to-server authentication "is required for all hybrid scenarios except hybrid OneDrive" (plan SharePoint Server hybrid, checked on 13 November 2026). When search and taxonomy fail together while the OneDrive link still redirects, we would look at the trust first.

Prerequisites

- **A baseline**: the Validation Checklist completed when each feature was configured (Chapters 2 to 6), and the Certificate Register from Chapter 2.
- **Certificate notification contacts.** One health rule exists only to say they are missing: "Certificate notification contacts haven't been configured" (health analyzer rules for SSL certificates, checked on 13 November 2026).
- **A test farm at the production build**, connected to a test tenant. What Microsoft leaves unsaid is settled only there.
- **Pilot accounts**: a synchronised, licensed user inside each hybrid audience and one outside (Chapter 4).

Decision criteria

How often to patch. Microsoft's floor is the servicing rule below. We would install each month's update on the test farm, run the validation set there, and follow in production within the month: the farm carries a trust into the tenant, and the security updates protect it.

Which release ring. We would leave production on Standard, the default, and put the test farm on Early, so that a hybrid change shows there first.

What counts as a hybrid change. Any change to the realm, the STS certificate, the synchronisation tool or the farm's update level, whoever raises it. Microsoft ties each to hybrid: the realm "must always match"; a replaced certificate needs "additional steps required to upload the STS certificate to Azure" (replace the STS certificate); synchronisation stops below a version; and an update can switch a hybrid feature on by ring. We would add the release ring, the outbound firewall rules and the timer service account. Each such change runs the validation set before and after.

Procedure

Microsoft documents no operating procedure for hybrid. This one is assembled from the servicing pages and the earlier chapters' checks.

Patch management

The rule. "Microsoft releases new Public Update (PU) builds for SharePoint Server Subscription Edition each month", "each PU build will be supported for one year from its release date", and "Support for a PU build ends on the second Tuesday of the same month of its release in the following year" (Subscription Edition servicing policy). On an older build, "you might be required to upgrade to a supported build before the Microsoft Support team can offer any further assistance".

The notices. From Version 24H2 the farm tells you. Six months before the date it shows "an **informational** notice in Central Administration and the SharePoint Management Shell"; three months before, "a **warning notice**"; beyond it, an error that "also appears in the Windows Application Event Log" (Version 24H2, checked on 13 November 2026).

The update. Since March 2023 it is "a single "uber" patch" each month, and installing it is half the work: updating "is a two-phase process: patching and build-to-build upgrade" (software updates overview, checked on 13 November 2026). The list of updates, with builds and dates, is SharePoint updates (checked on 13 November 2026). Chapter 1 works out which builds are still supported, and Chapter 42 has the procedure.

Zero downtime patching. It "is available in SharePoint Server 2016, SharePoint Server 2019, and SharePoint Server Subscription Edition", and "A highly available SharePoint Server farm *is* a requirement for ZDP." The commands run "one server at a time and not in parallel", and Microsoft says to "consider stopping Search crawls and Profile Imports during the upgrade or patch window" (zero downtime patching steps, checked on 13 November 2026). The page says nothing about hybrid. We do not know how the cloud crawl, taxonomy replication or the redirects behave while half the farm is on the new build. The test is one patch of the test farm with the cloud crawls paused, timing the taxonomy job and a pilot redirect.

Release rings. "Standard release is the default feature release ring." Early release features "are supported for production use but may change", and after changing ring "you must run the SharePoint Products Configuration Wizard on every server" (Version 22H2, checked on 13 November 2026). From Version 23H2 the ring is read with `Get-SPFeatureReleasePreference` and set with `Set-SPFeatureReleasePreference -FeatureReleaseRing {Early | Standard}` (Version 23H2, checked on 13 November 2026). The ring has decided hybrid once: the new cloud hybrid search shipped to the Early ring first, and the update of 8 July 2025 "Enables flight for the new Hybrid Search feature in the Standard release ring" (KB 5002751, checked on 13 November 2026). Chapter 3 has the detail. Record the ring beside the build.

Monitoring

The only health analyzer rules near this subject are the four for SSL certificates, and Microsoft does not say they cover the STS signing certificate: until one has reported it on your farm, assume none will. Whether a failed run of `Taxonomy Groups Replication` is surfaced anywhere is not established. So hybrid is watched by hand. "Documented" marks Microsoft's own check; "our test", one assembled from documented tools.

CHECK	TOOL	EXPECTED	KIND
Build support	The notice in Central Administration; the build against SharePoint updates	No notice, or the informational one	Documented
SSL certificates	"Upcoming SSL certificate expirations", weekly, "within the next 15 - 60 days"; "SSL certificates are about to expire", daily, "within the next 15 days"; "SSL certificates have expired", daily, "within the past 15 days"	No rule firing. The thresholds are "configurable"	Documented, for SSL certificates in use
The STS certificate and its copy in the tenant	Chapter 2's script; the principal's `KeyCredentials`	The thumbprint and end dates in the register	Our test
The realm and the trusted token issuer	`Get-SPAuthenticationRealm` against the tenant's ID; `Get-SPTrustedSecurityTokenIssuer`	"These GUIDs should be identical."; **RegisteredIssuerName** is `00000001-0000-0000-c000-000000000000@<context ID>`, where the first part is Microsoft's own identifier for the Azure Access Control Service, the same in every tenant	Documented
The hybrid link settings	`Get-SPO365LinkSettings` (checked on 13 November 2026)	The same output as the last run	Documented cmdlet; the comparison is ours
The cloud crawl	The cloud Search service application's crawl log, with its **online ID** column and **Warning breakdown** pivot	Crawls completing; no new class of error or warning	Documented log; our routine
On-premises items in the tenant's index	The query `IsExternalContent:true`, also written `IsExternalContent:1`	A count near the last, with a recent item in it	Documented query; the trend is ours
Taxonomy replication	The last run of `Taxonomy Groups Replication` in Central Administration; a test term added in Microsoft 365	A run within the day, since the job "performs a daily update of changes and a weekly full replication"; the term on the farm	Our test
Each redirected link	A pilot user selects OneDrive, their profile, Sites, Follow and the site creation page	Chapter 4's matrix	Documented for OneDrive and Follow; the rest ours
Federated search	A federated user searches on the farm	Two result blocks (Chapter 3)	Documented
Directory synchronisation	The installed Microsoft Entra Connect Sync version against the version history; the time of its last successful synchronisation	A supported version; "version 2.6.84.0 or later" with "application-based authentication by April 7, 2027"	Documented dates; the comparison is ours

Sources not yet cited: new in Subscription Edition, configure cloud hybrid search and plan hybrid taxonomy, checked on 13 November 2026.

The `Get-SPO365LinkSettings` reference lists the cmdlet as applicable up to SharePoint Server 2019, while the wizard checks for it on every version (Chapter 2): confirm it on your build.

Ownership and change

The assignments are ours; Microsoft documents roles for configuration (Chapter 2), not for operations. R does the work, A answers for it, C is consulted, I is informed.

ACTIVITY	FARM ADMINISTRATORS	IDENTITY TEAM	MICROSOFT 365 ADMINISTRATORS	SECURITY	SERVICE OWNER
Public updates and the validation set after each	R	I	I	C	A
Realm, trusted token issuer and proxies	R	I	C	C	A
STS certificate and its upload to the tenant	R	I	R	C	A
Synchronisation tool: version and authentication method	C	R	C	I	A
Privileged sessions in the tenant	C	I	R	A	I
Monitoring, validation, incidents and rehearsals	R	C	C	C	A

The change rule binds all five: a change raised by the identity team or by security is tested for hybrid by the farm administrators, and the service owner signs.

Verify

Microsoft documents a test at the end of each feature's configuration, and none to repeat later. This cadence is ours.

WHEN	WHAT TO REPEAT
Daily	The cloud crawl log, for new errors and warnings. The last run of `Taxonomy Groups Replication`. The health analyzer, where two certificate rules run daily
Weekly	The `IsExternalContent:true` count. One redirected link as each pilot user. The weekly certificate rule and the week's full taxonomy replication
Monthly	The build against SharePoint updates, and the notice. Chapter 2's read-only script, compared with last month's output. The Certificate Register. The synchronisation tool's version against the version history
After each public update	The whole set, on the test farm and then in production: the trust's reads, every redirect inside and outside the audience, a crawl and the query, a term round trip, the two federated result blocks, Chapter 6's trimming test, and every add-in
After each network or certificate change	Network: a crawl of a small content source through the real outbound path, the query, a redirect and a manual taxonomy run. Certificate: the trust's reads, the copy on the tenant's principal, and a hybrid query before and after
After a change to the synchronisation tool	A newly created pilot account that reaches Microsoft 365, is licensed, and gets trimmed results and a working redirect

Keep each result, dated and signed.

When it fails

SYMPTOM	DOCUMENTED CAUSE	FIRST CHECK	DETAIL
Every trust-dependent feature fails at once	The realm no longer matches the tenant's ID. Or the STS certificate was replaced without the upload: the requirement is documented, the symptom is not	`Get-SPAuthenticationRealm`; the STS thumbprint against the tenant's principal; then the outbound path	Chapter 2
On-premises results missing from Microsoft 365	Crawls failing over TLS 1.0 or 1.1, with "An existing connection was forcibly closed."; the quota, with "HTTP status: Forbidden" in the crawl log; for one person, access through Domain Users or an account that is not synchronised	The crawl log; then the query as a user with direct access	Chapter 3
Farm search shows only local results	The Search service application proxy "deployed in partition mode", with an OAuth2 "(404) Not Found" in the ULS log; the article names SharePoint 2013	The proxy	Chapter 3
Terms not arriving	None documented for replication. A stated requirement: the timer service account "must be a term store admin in SharePoint Server". Or replication was stopped	The job's last run; the **Term Store Administrators** box	Chapter 5
A redirected link fails for one user	No troubleshooting page. The configuration pages name the audience, the licence and the browser cache	The user against the audience and the licence; then wait 24 hours	Chapter 4
A redirected link fails for all	None documented	`Get-SPO365LinkSettings` against the last output; the selection in Central Administration	Chapter 4
Add-ins return HTTP 401 after a change	The realm changed; token issuers are tied to the old one	The realm before and after; the repair in KB 4010011	Chapter 2

Sources: hybrid search failures, cloud hybrid search FAQ, online content not displayed, configure hybrid taxonomy and KB 4010011, all checked on 13 November 2026.

The documented diagnostics are few, and all are for search. The TLS page says: "Starting on June 30, 2021, the Search service will no longer accept connections that use TLS 1.1 or 1.0"; its fixes name 2013, 2016 and 2019, not Subscription Edition. The FAQ names a ULS category, "Crawler:Azure Plugin" at VerboseEx, and a counter set, "Search Gatherer Azure Plugin - SharePointServerSearch". Both were written before the service changed in 2025, and we do not know whether either name survives. The test is `Get-Counter -ListSet` with that name on a search server. For the trust, the redirects and taxonomy replication, Microsoft names no ULS category and no counter. A problem that outlasts its first check goes to the test farm, then to Microsoft Support.

Security

The certificate that does not expire, and the one that does. "The default STS certificate does not need to be renewed. Renewal only applies after the STS certificate has been replaced." (replace the STS certificate). A farm that kept the default has no renewal to schedule, only the end date on the tenant's copy to record (Chapter 2). A replacement will "expire within 1 to 3 years", is replaced "on every server in the farm", and must then be uploaded to the tenant again. For that upload Microsoft points to an add-in article whose function depends on a deprecated module, and no page says which procedure is the hybrid renewal: Chapter 2 holds the gap and the route we would rehearse. In operations: the register carries the date, the renewal is rehearsed on the test farm a cycle ahead, and a hybrid query is run before and after.

Privilege. Onboarding search again and running the wizard again ask for a Global Administrator (Chapters 3 and 5). Chapter 6's rule holds: the role is held for the session and recorded.

Rollback and recovery

Switching a feature off, as documented. Microsoft's removal page is the whole of it (removing SharePoint hybrid scenarios, checked on 13 November 2026):

- **Cloud hybrid search**: delete the content sources, then the Search service application. To clear what is already indexed, "contact the support team for further guidance" (Chapter 3).
- **OneDrive and sites features**: in Central Administration, on **Configure hybrid OneDrive and Sites features**, select **None**, which "also removes the Hybrid app launcher feature" (Chapter 4).
- **Taxonomy and content types**: `Stop-SPTaxonomyReplication` and `Stop-SPContentTypeReplication`; to start again, "you must run the Hybrid Configuration Wizard again" (Chapter 5).
- **The trust**: last, the two service application proxies and an `iisreset` on every server (Chapter 2).

The wizard is never the way back: it "doesn't uninstall features. If you run the Hybrid Configuration Wizard and deselect a feature that you previously installed, it remains installed." (Hybrid Configuration Wizard, checked on 13 November 2026). Chapter 8 has the order. In an incident, switching a feature off stops the symptom and removes nothing already sent.

Restoring the farm. None of the hybrid pages we read mentions backup or restore, and none says what a restored farm does to the trust. The realm, the proxies and the STS certificate are configuration, and whether they survive even a database attach is not established (Chapter 2). We do not know whether a restored farm still holds the realm and the certificate whose public key the tenant holds, or whether the redirects and the timer job return. The rehearsal settles it:

1. Restore the farm to recovery hardware.
2. Before any crawl starts, run Chapter 2's read-only script and compare the realm, the trusted token issuer, the STS thumbprint and the hybrid link settings with production's last output.
3. Run one hybrid query, one redirect per pilot user and one manual taxonomy replication.
4. Record what had to be rebuilt and how long it took. That list is the recovery procedure.

Do not let the restored farm crawl during the rehearsal: "crawling the same source content from multiple Cloud SSA farms connected to the same Microsoft 365 organization **is not supported**" (cloud hybrid search FAQ). A recreated cloud Search service application starts from a full crawl (Chapter 3). For a term store restored from an older backup, we do not know whether the next full replication reconciles it: run the job and compare a replicated group with Microsoft 365.

Working documents

The Hybrid Architecture Advisor generates these in the browser from your answers about the farm. What you did not answer is left as unknown, never filled in.

- **Operations Runbook (Word).** The patch rhythm, the ownership table with your names, the change rule, the incident table, and the **recovery procedure**: the documented switch-off for each feature you run and the restore rehearsal.
- **Monitoring Checklist (Excel).** One row per check in the monitoring table, marked documented or own test, with its frequency, owner and last result.
- **Validation Checklist (Excel), operations rows.** The cadence table as rows to repeat, each with who ran it, when and what they saw.

Sources

- Updated Product Servicing Policy for SharePoint Server Subscription Edition, checked on 13 November 2026
- Configure server-to-server authentication from SharePoint Server to SharePoint in Microsoft 365, checked on 13 November 2026
- Replace the STS certificate for SharePoint Server, checked on 13 November 2026
- Microsoft Entra Connect: Version release history, checked on 13 November 2026
- Plan SharePoint Server hybrid, checked on 13 November 2026
- New health analyzer rules for SSL certificates, checked on 13 November 2026
- New and improved features in SharePoint Server Subscription Edition Version 24H2, checked on 13 November 2026
- Software updates overview for SharePoint Server 2016, 2019, and Subscription Edition, checked on 13 November 2026
- SharePoint updates, checked on 13 November 2026
- SharePoint Server zero downtime patching steps, checked on 13 November 2026
- New and improved features in SharePoint Server Subscription Edition Version 22H2, checked on 13 November 2026
- New and improved features in SharePoint Server Subscription Edition Version 23H2, checked on 13 November 2026
- Description of the security update for SharePoint Server Subscription Edition: July 8, 2025 (KB5002751), checked on 13 November 2026
- Get-SPO365LinkSettings, checked on 13 November 2026
- New and improved features in SharePoint Server Subscription Edition, checked on 13 November 2026
- Configure cloud hybrid search - roadmap, checked on 13 November 2026
- Plan hybrid SharePoint in Microsoft 365 taxonomy and hybrid content types, checked on 13 November 2026
- Hybrid search fails to crawl or return results, checked on 13 November 2026
- Cloud hybrid search service (Cloud SSA) FAQ, checked on 13 November 2026
- SharePoint Online content isn't displayed in a SharePoint on-premises search, checked on 13 November 2026
- Configure hybrid SharePoint taxonomy and hybrid content types, checked on 13 November 2026
- Provider-hosted add-ins stop working and HTTP 401 error after you configure SharePoint farm hybrid features (KB 4010011), checked on 13 November 2026
- Removing SharePoint hybrid scenarios, checked on 13 November 2026
- Hybrid Configuration Wizard in the SharePoint admin center, checked on 13 November 2026

Related pages on this site

- Chapter 2 of this guide: the trust and the Certificate Register.
- Chapter 3, Chapter 4 and Chapter 5: search, the redirects and taxonomy.
- Chapter 6: the governance control matrix.
- Chapter 8: the exit, and the order of removal.
- SharePoint Migration Field Guide, Chapter 42: keeping Subscription Edition supported, one update at a time.
- Install a Subscription Edition update without downtime.
- SharePoint Server security updates, end of support dates and Microsoft 365 endpoints.
- Hybrid Architecture Advisor.

Before you continue

- [ ] The farm is on a supported public update, its release ring is recorded, and the patch rhythm has a named owner
- [ ] Every row of the monitoring table has an owner, a frequency and a first result, and is marked as Microsoft's check or your own test
- [ ] The Certificate Register shows whether the STS certificate is the default or a replacement, with its end dates, and the synchronisation tool's version is recorded against 2.6.84.0 and 7 April 2027
- [ ] The validation set has been run after a public update on the test farm, and its results are kept
- [ ] Each symptom in the incident table has a first check that somebody on call can run
- [ ] A change to the realm, the STS certificate, the synchronisation tool or the update level is treated as a hybrid change, with a named approver
- [ ] The switch-off for each feature and the restore of the farm have been rehearsed, and the list of what had to be rebuilt is written down