Architecture approaches for Microsoft cloud tenant-to-tenant migrations

This series of topics illustrates several architecture approaches for mergers, acquisitions, divestitures, and other scenarios that might lead you to migrate to a new cloud tenant. These topics provide starting-point guidance for planning.

Most customers work with Microsoft Consulting Services or a Microsoft partner to migrate tenants, including using third-party tools to migrate content. In the examples provided in these topics, Contoso is the source tenant and Fabrikam is the target (destination) tenant.

Business scenario	Architecture scenario	Architecture approach
I sold a business unit and brand identity Contoso users will continue to be known as *user*@contoso.com.	**Tenant-to-tenant migration without rebranding** Identities will migrate to a target Active Directory and tenant, and will keep the existing domain as part of the migration.	**Single-event migration** Almost everything is migrated in a single event. Higher risk, shorter timeline. Avoid single-event migrations larger than 15,000 users or 7 TB of site content. Data volumes, network bandwidth, and helpdesk capacity can be limiting factors to scale. Consider using an alternate temporary domain for a phased migration if you are unable to accommodate a single event.
I sold a business unit and the business unit will adopt the target company's branding Contoso users will be known as *user*@fabrikam.com.	**Tenant-to-tenant migration with rebranding** Identities will migrate to a new target Active Directory and tenant and will change the brand identity as part of the migration.	Choose one **Phased migration** Gradual migration of users, services, and data. Source domains are not transferred. Users assume new target domains. Lower risk, longer timeline. Coexistence limitations can cause issues.
I need to split users across two tenants **My company cannot use the registered (*.onmicrosoft.com) tenant name** **I'm moving from a commercial tenant to Microsoft Cloud for Government**	**Cloud tenant move** Identities remain in the source Active Directory, but I'm moving all workloads to a new cloud tenant for all users in the affected domain.	**Tenant move or split** Similar to single-event migration, except this does not include migrating accounts to a new Active Directory forest. For tenant splits, this approach is not intended for long-term coexistence. Migration event includes additional work to re-establish existing identities to the new tenant.

Technical questions

- Do you need to retain the domain in the target environment? (How do you want to be known by the outside world in the end-state?)
- Are you migrating to a brand new environment (greenfield), or targeting an existing Active Directory environment and tenant?
- What type of continued collaboration between environments is expected in the end-state?
- What workloads are being used in the source tenant?
- How many accounts are in scope?
- Is mail forwarding required after migration?
- Is a unified GAL required?

Non-technical questions

- How will you reconcile policy conflicts as they arise?
- Which project metrics are fixed and which can be optimized (time, resources, scope, quality, user experience)? For more information, see The project triangle.
- What are the "Day 1" requirements? Day two and beyond?

Migration events

Because both tenants and services are live at the same time, a user's migration can be thought of as a 'migration event.' The activities may vary, but include the following.

Prior to the migration event:

- Send communication to each user.
- Put mailboxes and content into read-only mode.

At the migration event:

- Stop reverse forwarding mail to allow new email to be delivered to the target
- Enable target accounts, if required.
- Complete the final data migration.

Post-migration event:

- Users must recreate their mobile profiles.
- Client software needs to be reconfigured (Outlook, OneDrive for Business Sync Client, Office ProPlus activation).

Architecture approaches for Microsoft cloud tenant-to-tenant migrations

Design considerations

Pre-stage vs dial-tone

You can pre-stage mailboxes and SharePoint and OneDrive content before the cut-over event (final domain name move), after the cut-over event, or a combination of the two.

Pre-stage content

If the timeline permits, pre-stage content prior to the migration event.

- Start with the oldest content first.
- Migration tools typically do not replicate mailbox data changes from source. For mailbox data, stop performing deltas for content under 30 days. For SharePoint and OneDrive, do incremental syncs as needed.
- Migration is complete after running the final delta sync, in conjunction with the final completion events.

Dial-tone

Right after cutting over to the new tenant, migrate a minimal amount of content. Continue to migrate content after the initial data migration.

- Requires continued access to the source.
- Useful if there's not enough time to pre-sync.
- Better network performance for the initial data migration content re-caching (as opposed to caching entire mailboxes over the network).
- Works best for mailbox data only. This approach leads to a poor user experience with OneDrive and SharePoint data migrations.

A typical strategy includes:

- One week of mail on the initial migration.
- One month of mail at the next milestone.
- Remaining mail at the final milestone.

SharePoint Online and OneDrive for Business migration

Aligning SharePoint and OneDrive for Business data requires careful planning.

- Data volumes can be quite large and, unlike mail data, the documents are frequently changing.
- In single event migrations, the required UPN changes during the migration will require re-mapping source to target.

Migrating Active Directory accounts to a new domain

Both architecture approaches involve moving user accounts from an existing domain to a target domain. There are several approaches you can take:

- Use third-party tools
- Hire Microsoft Consulting Services (Active Directory Migration Service)
- Hire a Microsoft partner

Be sure to plan which properties to migrate with the user accounts. For example, migrating the Exchange Legacy DN property allows users to reply to old emails.

Exchange hybrid configuration

Both approaches require an Exchange management server on-premises with hybrid connectivity. This is necessary to manage properties of the mailboxes and to forward email to the new tenant, if needed, in a phased migration. Consider running the minimal hybrid configuration option in the Exchange Hybrid Configuration Wizard (HCW) if you do not require additional functionality.

For more information, see How and when to decommission your on-premises Exchange servers in a hybrid deployment.

Migrating to an existing tenant

If the target Active Directory environment or tenant already exist, consider these additional complexities:

- The naming format for users might change as well as the domain to match an existing policy.
- How will policy conflicts be resolved?
- Does the target tenant have access restrictions (for example, Azure AD conditional access policies) that may prevent access from migrated identities?

Long term tenant co-existence

If required, ongoing collaboration may be required between tenants. See Office 365 inter-tenant collaboration.

Current tenant-to-tenant workload migration capabilities

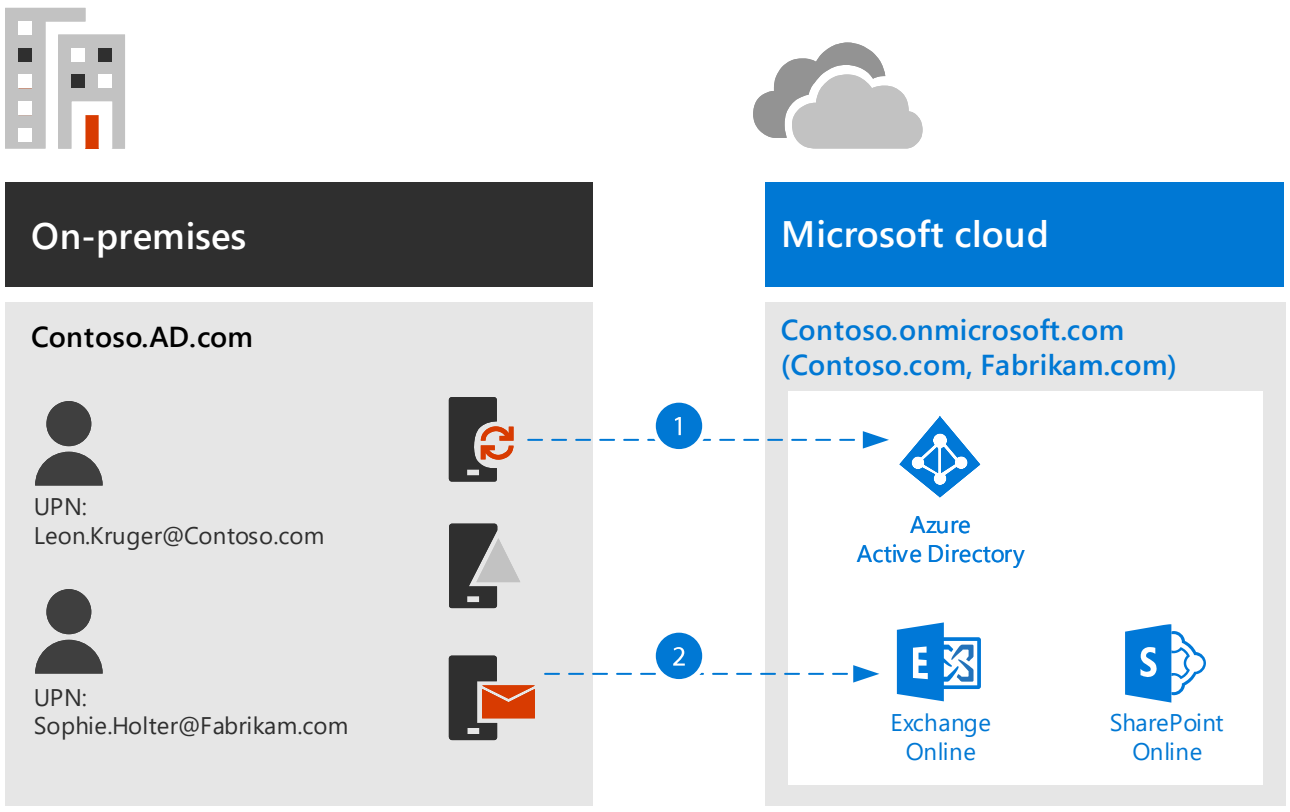
Service	Can migrate	Notes
Office ProPlus	Yes	See Reset Office 365 ProPlus activation state
Exchange mailboxes	Yes	Microsoft Consulting Services (MCS) and/or third-party tool
Exchange public folders	Yes	MCS and/or third-party tool
SharePoint sites	Yes	MCS and/or third-party tool
OneDrive for Business folders	Yes	MCS and/or third-party tool
Office 365 groups	Yes	MCS and/or third-party tool
Teams	Partial	Content migration requires 3rd party tool Scripts to recreate the Teams structure and permissions
Yammer	Partial	Limited scenarios supported – requires a service ticket with Microsoft Support
Azure Information Protection	Partial	Limited scenarios supported – requires a service ticket with Microsoft Support. Labels cannot be migrated across tenants.
Stream	No	
Flow	No	
PowerApps	No	
PowerBI	No	
Intune	Yes	Manually recreate configuration. Mobile devices will require re-enrollment.

Architecture approaches for Microsoft cloud tenant-to-tenant migrations

Single-event migration

In this example, Contoso holds multiple brands, including Fabrikam. Fabrikam is moving to a new tenant. Migration events take place during a single time period, such as over a weekend.

Initial state



1. Contoso synchronizes identities with Azure AD Connect (AAD Connect).
2. Contoso retains an Exchange management server on premises with hybrid connectivity.

Note: Contoso.com is the primary domain. Fabrikam.com is an added custom domain in the existing, source environment.

Pre-cutover event

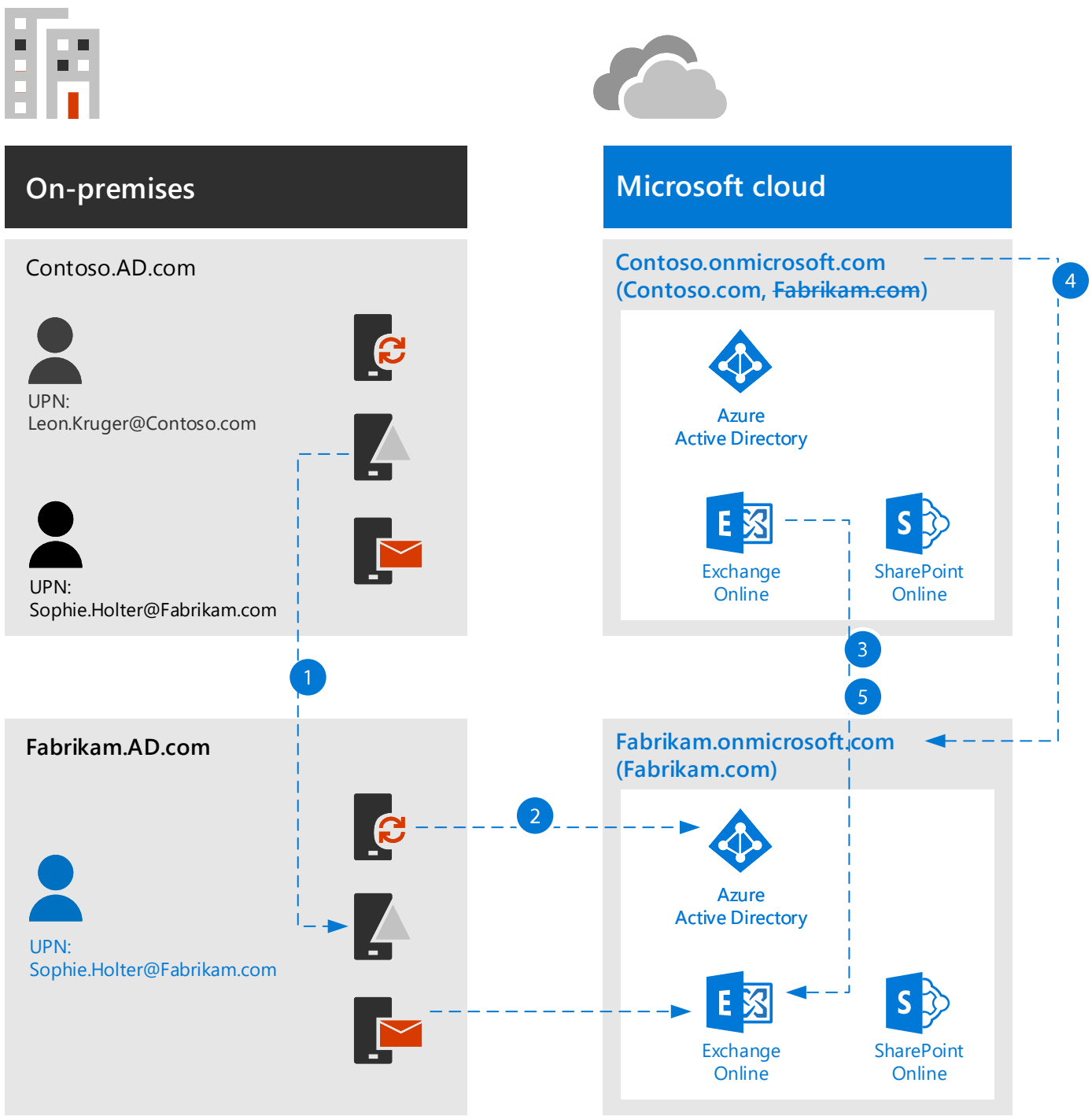
1. Replicate identities in the existing Active Directory domain (Contoso) to the target Active Directory domain (Fabrikam).

   If identities in the source domain are using the same UPN in the target domain, assign a temporary UPN.

2. Synchronize identities from the target Active Directory domain to the target Azure Active Directory tenant. Initially, the UPN will be the onmicrosoft.com domain.
3. Execute pre-stage content migration

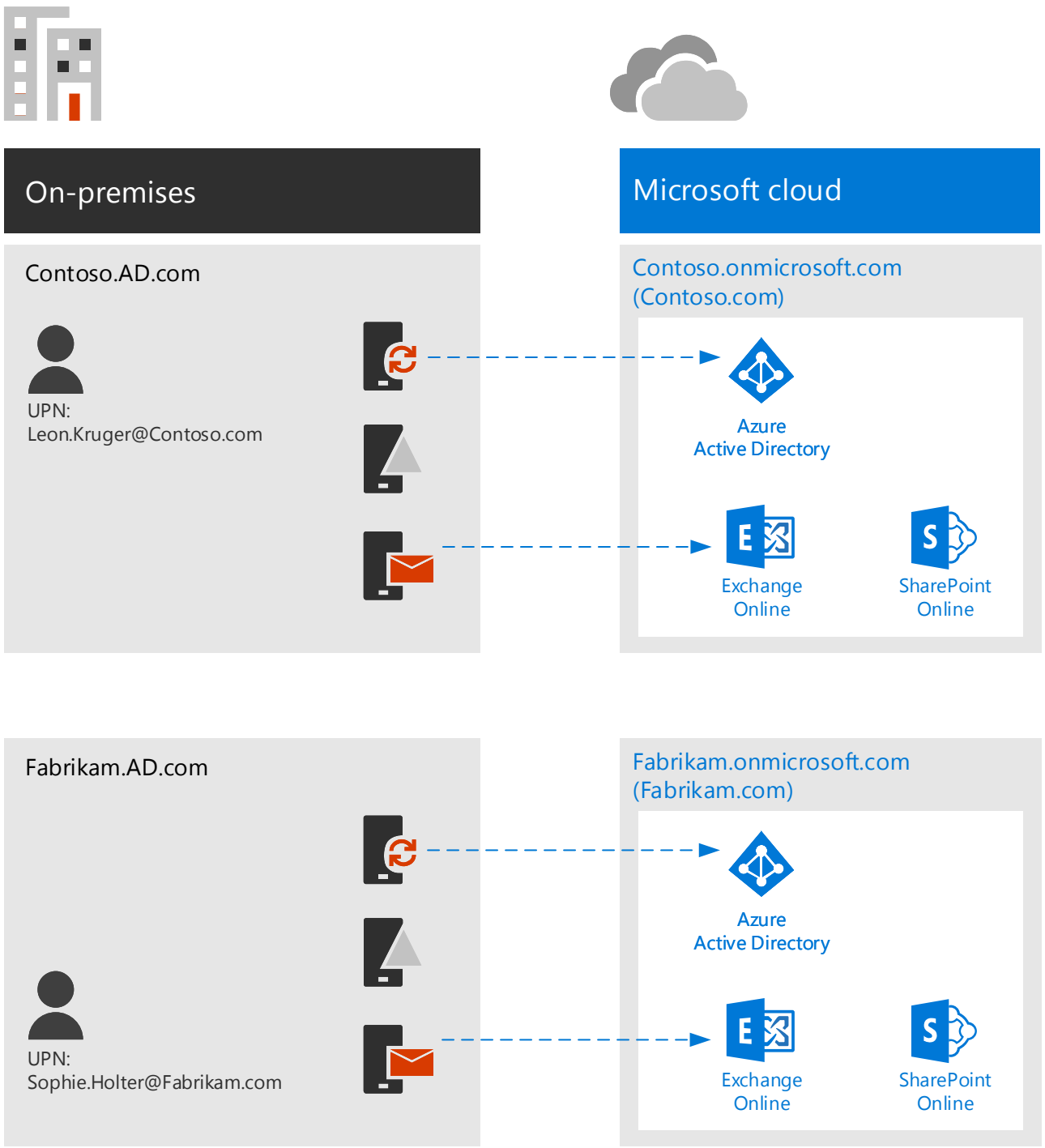
Cutover event

4. Prepare the target tenant (Fabrikam.onmicrosoft.com).
   - Remove the domain from all objects in the source tenant (Contoso). This includes SIP adresses, email addresses, proxy addresses, groups, and public folders.
   - Verify the domain on the target tenant (Fabrikam).
   - Assign the correct UPNs (Fabrikam) for users on the target UPNs. This will flow to the target tenant and replace the default onmicrosoft.com domain.
5. Perform completion events for each workload.



Continued on next page

End state



Cleanup:

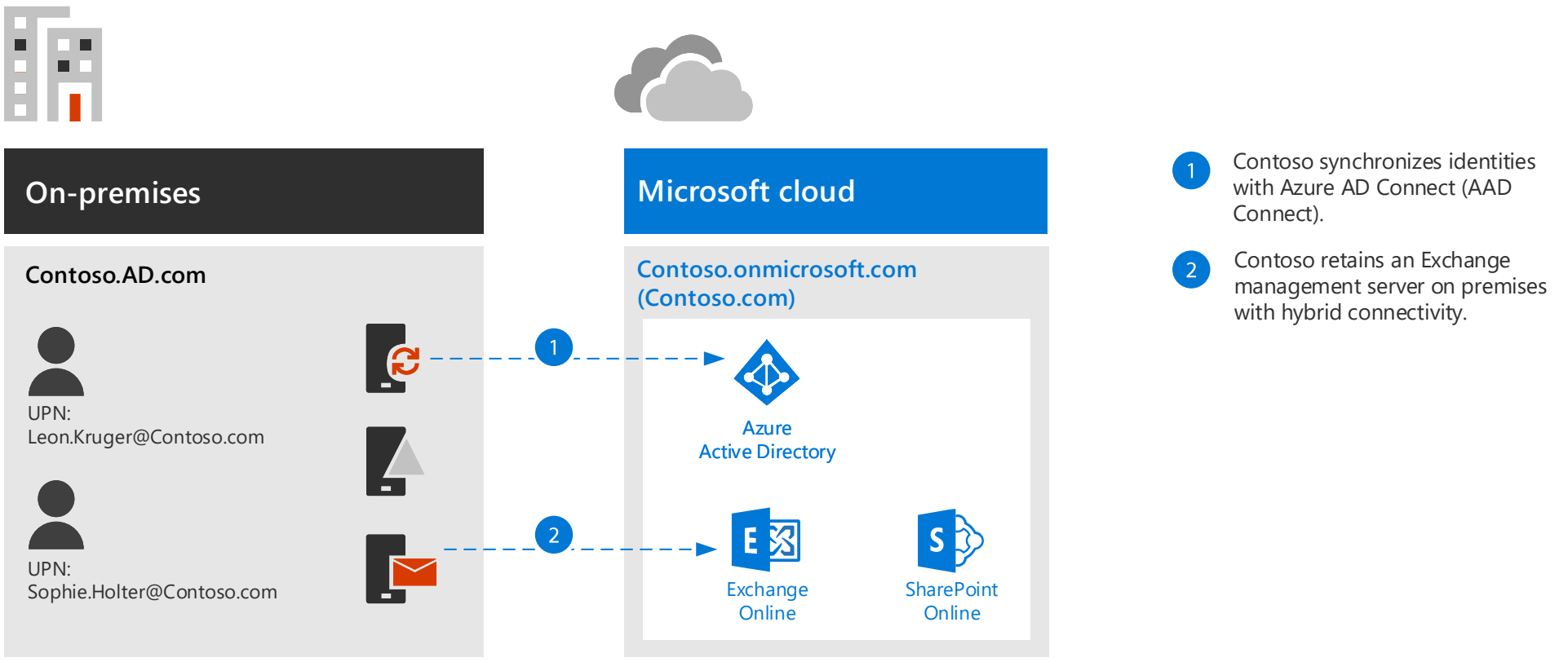
- Remove the migrated identities from the source domain (Contoso.com), if mail forwarding is not required. You can create a contact object if forwarding is still required.
- If an ongoing collaboration relationship is required, consider using Azure B2B between tenants.

Architecture approaches for Microsoft cloud tenant-to-tenant migrations

Phased migration

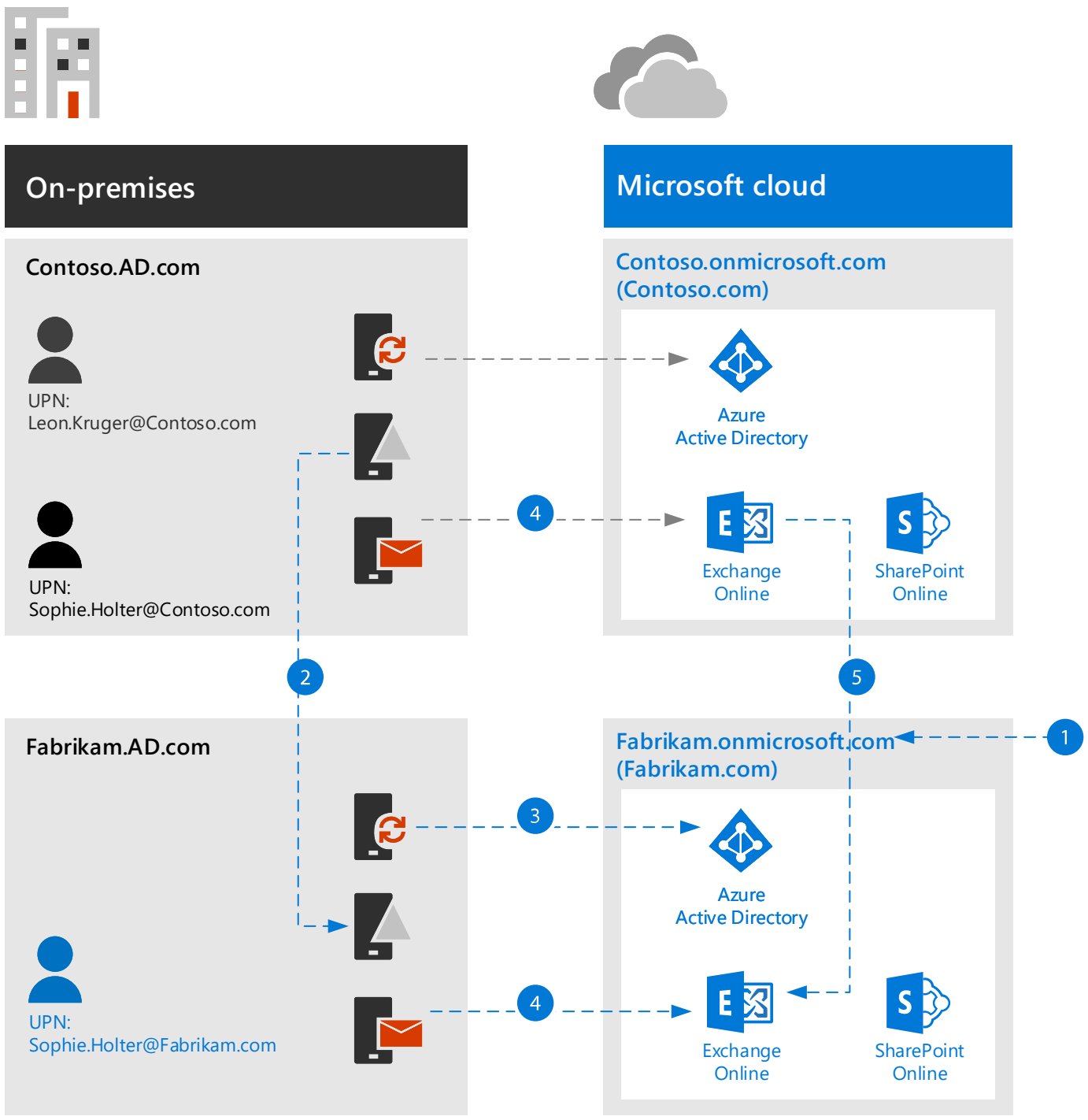
In this example, Contoso holds multiple brands, including Fabrikam. Fabrikam is moving to a new tenant. Migration events are phased over a longer period of time. While this approach works better for larger migrations, coexistence issues can be challenging.

Initial state



1. Contoso synchronizes identities with Azure AD Connect (AAD Connect).
2. Contoso retains an Exchange management server on premises with hybrid connectivity.

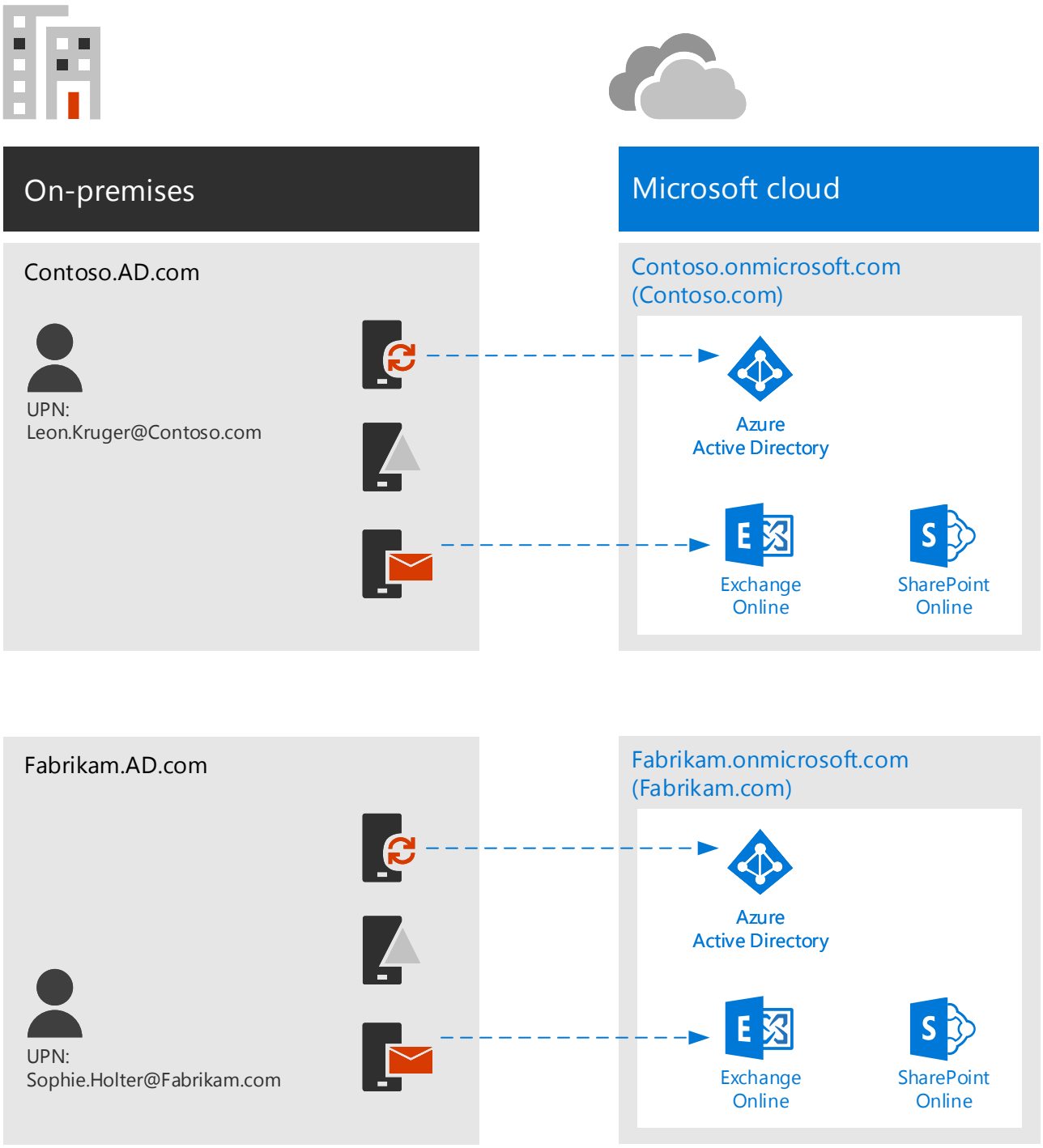
Bridge state



1. Prepare the target tenant (Fabrikam.onmicrosoft.com).
   - Verify the domain on the target tenant (Fabrikam).
   - Licenses must be available for both tenants.
2. Replicate identities in the existing Active Directory domain (Contoso) to the target Active Directory domain (Fabrikam).
3. Synchronize identities from the target Active Directory domain to the target Azure Active Directory tenant. Many customers disable user accounts until the user mailbox is migrated, however this will by default block the account from Office 365 access.
4. Enable forwarding and reverse forwarding SMTP.
5. Phased migration — Migrate user mailboxes to the new tenant. Remove reverse forwarding.

Continued on next page

End state



Cleanup:

- Remove the migrated identities from the source domain (Remainco.com), if mail forwarding is not required. You can create a contact object if forwarding is still required.
- If an ongoing collaboration relationship is required, consider using Azure B2B between tenants.

Coexistence challenges during phased migrations

User Experience Challenges

- Browser sessions can only authenticate to one tenant at a time.
- Skype contacts constantly changing.
- Single sign-on might make it difficult to access both tenants.
- Teams client confusion.
- Mail-enabled groups are challenging — during coexistence, replies to group threads are treated as Internet mail and may result in NDRs.

Move integrated services together whenever possible

Microsoft recommends moving services at the same time where there are strong dependencies between the services. For example, if you do not move Exchange and Skype together, you may experience errors scheduling Skype meetings and conversation might not be saved.

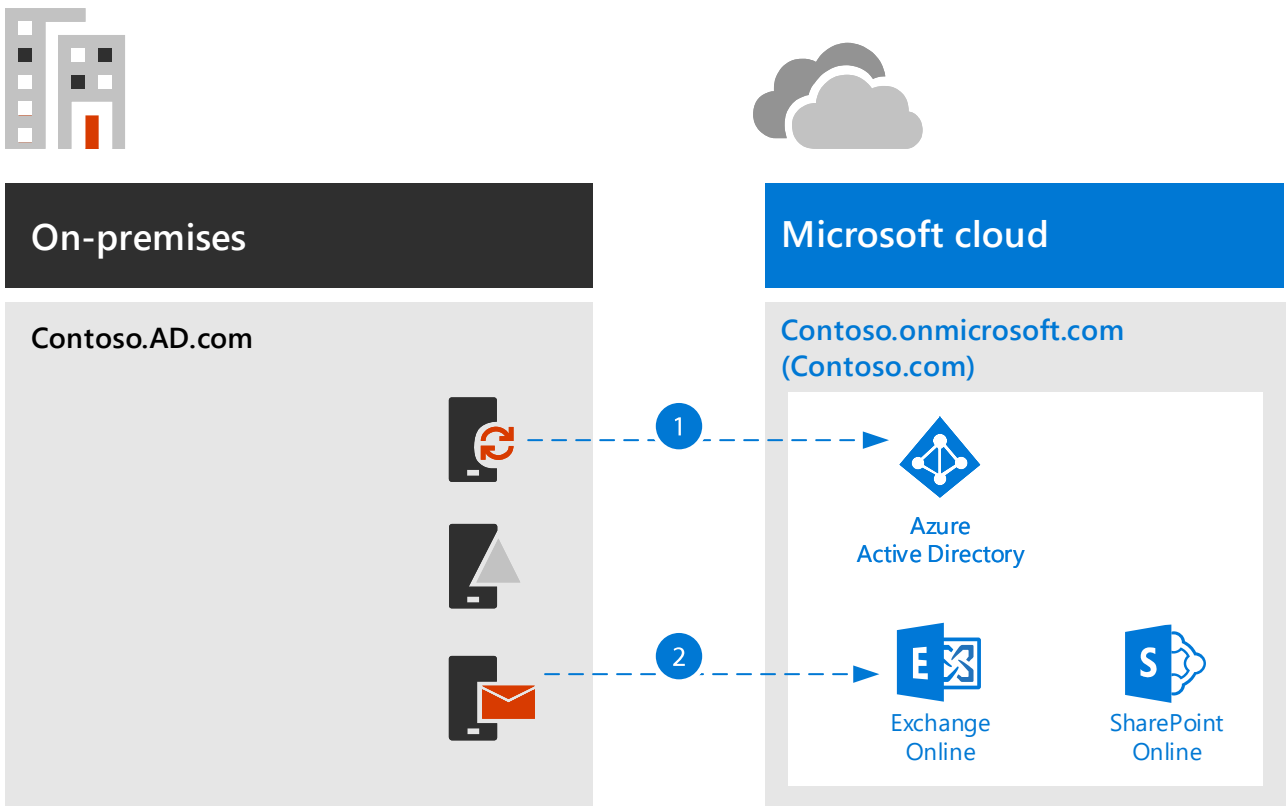
Architecture approaches for Microsoft cloud tenant-to-tenant migrations

Tenant move or split

In this example, Contoso is moving all users to a new tenant — Fabrikam. All users initially belong to the Contoso.com domain. Users are migrated from the Contoso.com domain to Fabrikam.com.

Not illustrated — moving a subset of user accounts to a new tenant.

Initial state



1. Contoso synchronizes identities with Azure AD Connect (AAD Connect).
2. Contoso retains an Exchange management server on premises with hybrid connectivity.

Note: If you are moving a subset of user accounts to a new tenant, separate these accounts using organizational units (OUs), groups, domains, or by using attributes.

Pre-cutover event

1. Prepare the target tenant (Fabrikam.onmicrosoft.com).
   - Create accounts in the target tenant. This can be accomplished by scripting or provisioning cloud accounts in the target tenant with a temporary UPN. Or, you can leave the default login (user@Fabrikam.onmicrosoft.com).
   - Licenses must be available for both tenants.
2. Pre-stage the content in the target tenant for each workload.

Cutover event

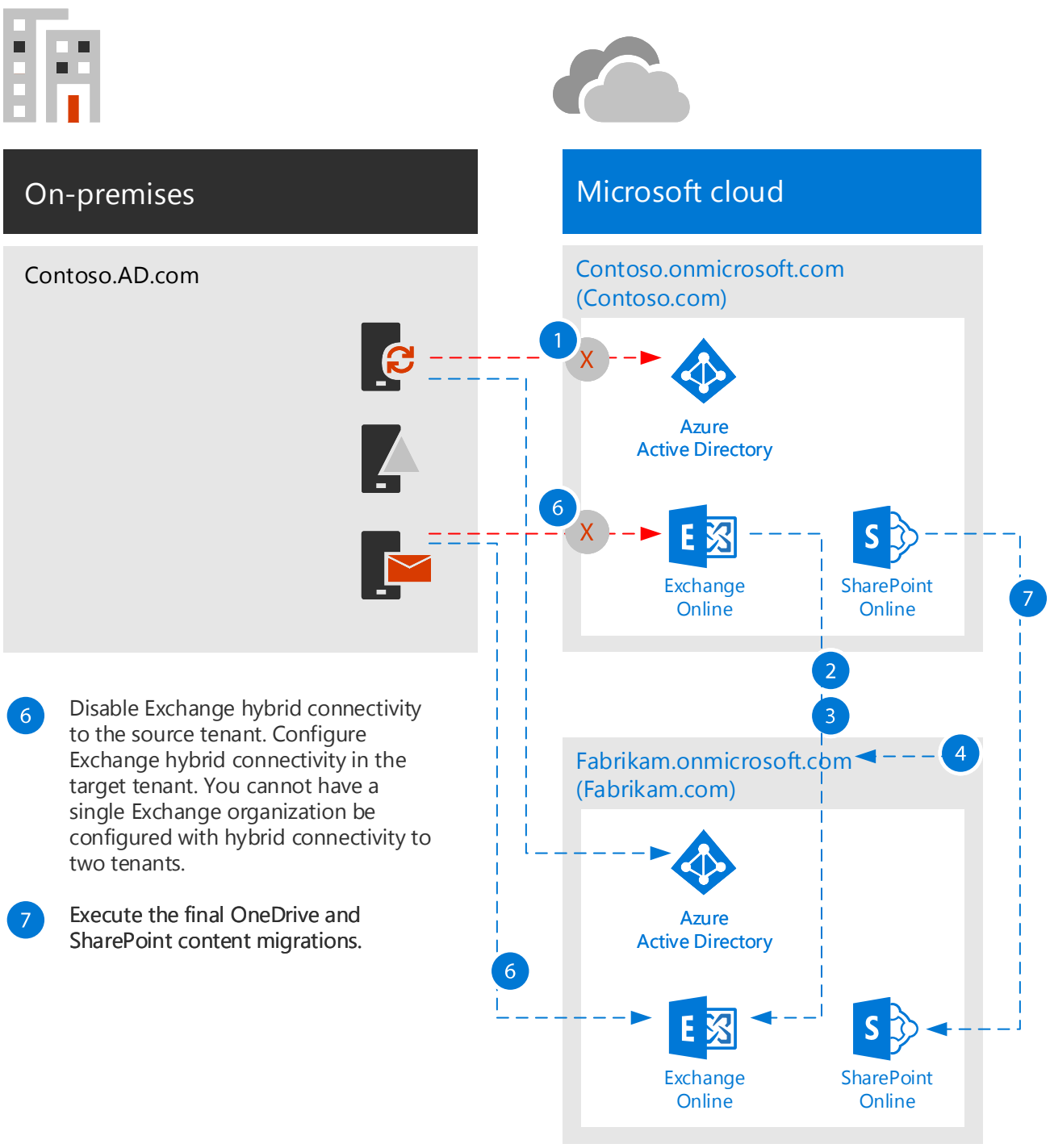
3. Execute the final content migration for email.
4. Initiate the domain transfer by removing the domain from all source objects.

   See sample scripts here: How to migrate mailboxes from one Office 365 tenant to another.

   Register and validate the domain on the target tenant.
5. Reinstall Azure AD Connect to point to the target tenant.

   Identities should soft-match with the target. See How to use SMTP matching to match on-premises user accounts to Office 365 user accounts for directory synchronization.

   Update Active Directory Federation Services (AD FS) if required.
6. Disable Exchange hybrid connectivity to the source tenant. Configure Exchange hybrid connectivity in the target tenant. You cannot have a single Exchange organization be configured with hybrid connectivity to two tenants.
7. Execute the final OneDrive and SharePoint content migrations.



Continued on next page

End state

At this point the source tenant is completely disconnected from Active Directory, and all content has been migrated to the target.

The organization can decommission the source tenant.

Note: If you are moving a subset of user accounts to a new tenant, the final architecture includes two Azure AD connect servers on premises, each synchronizing accounts to different Azure AD tenants.

The on-premises Exchange organization can be configured for hybrid connectivity with only one tenant.