Evaluating Requirements and Solutions for Identity Management

examlabpractice.com

https://t.me/learningnets

On-premises identity synchronization

- Microsoft recommends you have a good baseline and understanding of the issues in your on-premises environment that can result in synchronization issues to the cloud.
- Since automated tools such as IdFix and Azure AD Connect Health can generate a high volume of false positives, we recommend you identify synchronization errors that have been left unaddressed for more than 100 days by cleaning up those objects in error.
- Long term unresolved synchronization errors can generate support incidents. Troubleshooting errors during synchronization provides an overview of different types of sync errors, some of the possible scenarios that cause those errors and potential ways to fix the errors.

https://t.me/learningnets

Synchronization Scope and Object Filtering

Removing known buckets of objects that aren't required to be synchronized has the following operational benefits:

- Fewer sources of sync errors
- Faster sync cycles
- Less "garbage" to carry forward from on-premises, for example, pollution of the global address list for on-premises service accounts that aren't relevant in the cloud

Examples of objects to exclude are:

- Service Accounts that aren't used for cloud applications
- Groups that aren't meant to be used in cloud scenarios such as those used to grant access to resources
- Users or contacts that are external identities that are meant to be represented with Azure AD B2B Collaboration
- Computer Accounts where employees aren't meant to access cloud applications from, for example, servers

https://t.me/learningnets

Sync Failover or Disaster Recovery

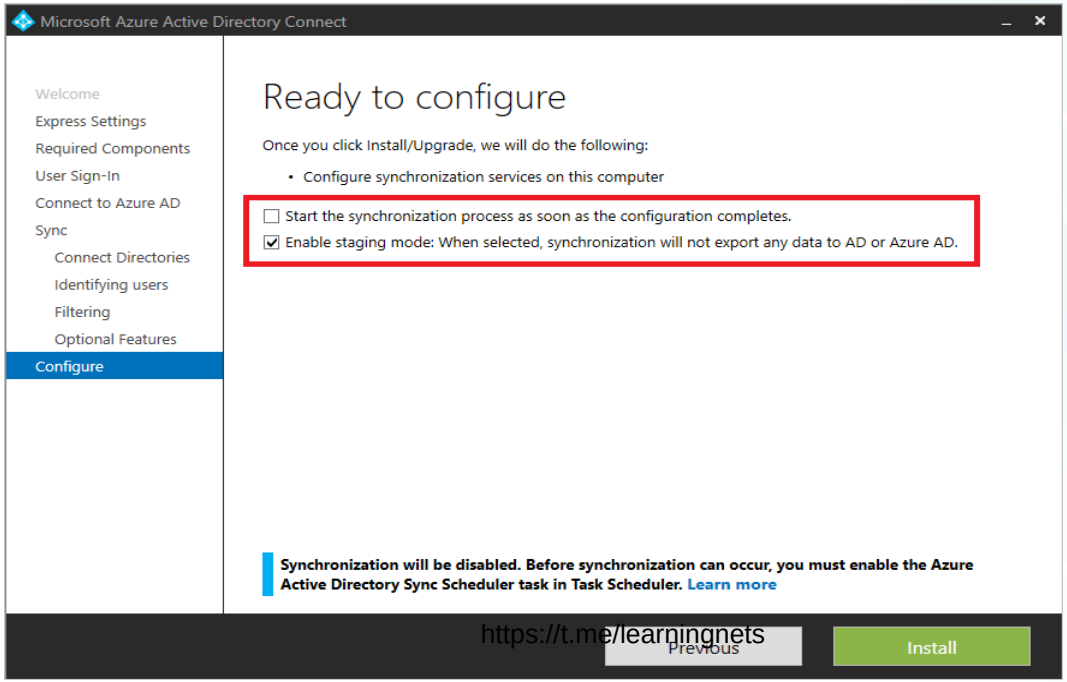
If the Azure AD Connect Sync Server goes offline for any reason, changes to on-premises cannot be updated in the cloud and can result in access issues for users. Therefore, it is important to define a failover strategy that allows administrators to quickly resume synchronization after the sync server goes offline. Such strategies may fall into the following categories:

- **Deploy Azure AD Connect Server(s) in Staging Mode** - allows an administrator to "promote" the staging server to production by a simple configuration switch.
- **Use Virtualization** - If the Azure AD connect is deployed in a virtual machine (VM), admins can leverage their virtualization stack to live migrate or quickly redeploy the VM and therefore resume synchronization.

https://t.me/learningnets

Enabling Staging Mode

If your organization is lacking a disaster recovery and failover strategy for Sync, you shouldn't hesitate to deploy Azure AD Connect in Staging Mode. Likewise, if there is a mismatch between your production and staging configuration, you should re-baseline Azure AD Connect staging mode to match the production configuration, including software versions and configurations.



https://t.me/learningnets

Source anchor

The sourceAnchor attribute is defined as an attribute immutable during the lifetime of an object. It uniquely identifies an object as being the same object on-premises and in Azure AD. The attribute is also called **immutableId** and the two names are used interchangeable.

The attribute is used for the following scenarios:

- When a new sync engine server is built, or rebuilt after a disaster recovery scenario, this attribute links existing objects in Azure AD with objects on-premises.
- If you move from a cloud-only identity to a synchronized identity model, then this attribute allows objects to "hard match" existing objects in Azure AD with on-premises objects.
- If you use federation, then this attribute together with the userPrincipalName is used in the claim to uniquely identify a user.

Using **ms-DS-consistencyguid** as the source anchor allows an easier migration of objects across forests and domains, which is common in AD Domain consolidation/cleanup, mergers, acquisitions, and divestitures.

https://t.me/learningnets