Planning Your Hybrid Identity Solution

Gary Grudzinskas
CLOUD ENGINEER AND AUTHOR

@garygrudzinskas

Objectives

Know what parts make up the Azure hybrid identity

Develop a plan to integrate your on-premises environment to the cloud

Design Principles

Your design should facilitate change

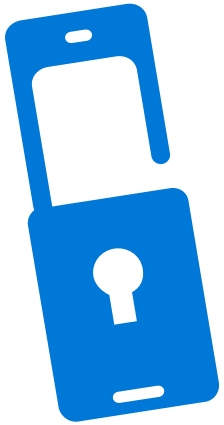
Hybrid identity starts as a supporting role and then unlocks more capabilities

Your design should leverage hybrid identity both on-premises and in the cloud

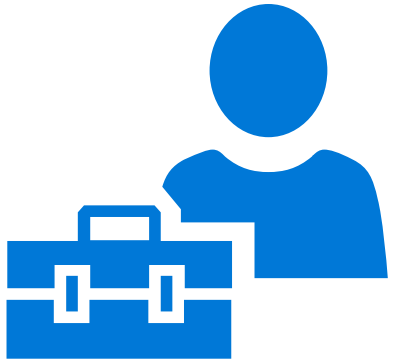
Your design should be scalable as the business needs grow and change

Planning for Sign On

Authentication and Authorization



Multi Factor Authentication



Delegation of Administration

Authentication and Authorization

How do users typically login to their on-premises environment?

How will users sign-on to the cloud?

Will you be allowing workers from partner networks access to cloud and on-premises resources?

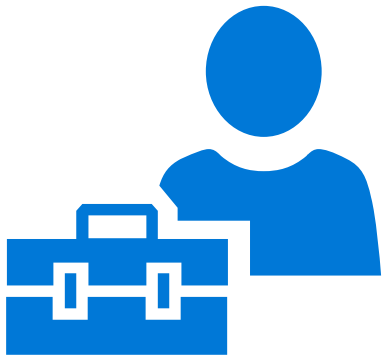
Multi Factor Authentication

Do you currently implement multi-factor authentication?

What are the key scenarios that you want to enable MFA for?

Will you use MFA to secure Microsoft apps?

Will you use MFA to secure remote access to on-premises apps?



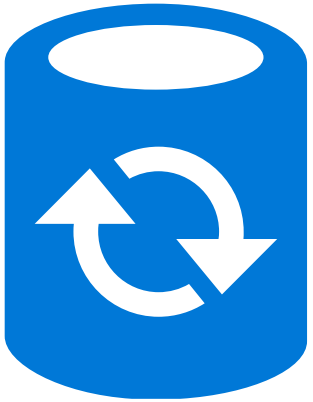
Delegation of Administration

Does your company have more than one user with elevated privilege to manage your identity system?

Does your company need to delegate access to users to manage specific resources?

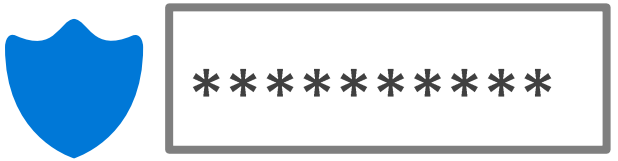
Does each delegated user need the same access?

Planning for Synchronization

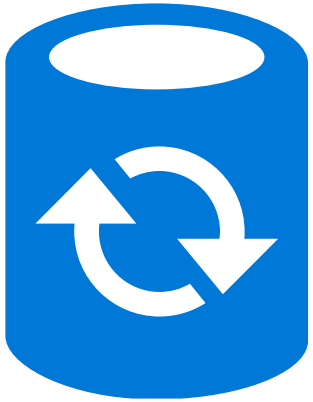


Directory Synchronization

Multi Forest Synchronization



Password Synchronization



Directory Synchronization

Do you have a disaster recovery plan for the synchronization server?

Where will the synchronization server be located?

Do you have any other directory on-premises like LDAP or an HR database?

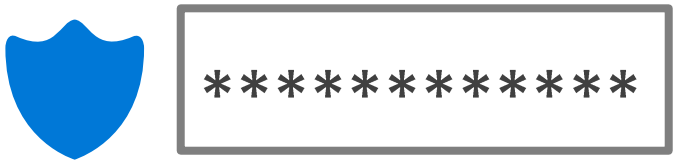
Does your company use Microsoft Exchange?

Multi Forest Synchronization

Are the UPNs unique in your organization?

Will the Azure AD Connect server be able to get to each forest?

Do you have an account with the correct permissions for all forests you want to synchronize with?



Password Synchronization

Do you have restrictions on storing passwords in the cloud?

Will your employees be able to reset their own passwords?

What account lockout policy does your company require?

Planning for Applications

Applications

Access Control

Applications

Will users be accessing on-premises applications? In the cloud? Or both?

Are there plans to develop new applications that will use cloud authentication?

Will cloud users be accessing applications on-premises?

Will on-premises users be accessing applications in the cloud?

Access Control

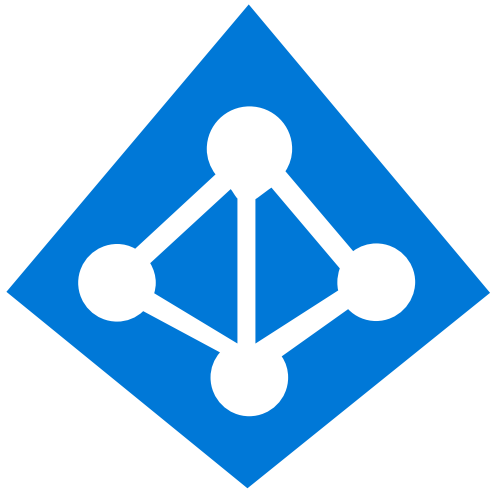
Does your company need to limit access to resources according to some conditions?

Does your company have any application that needs custom control access to some resources?

Does your company need to integrate access control capabilities between on-premises and cloud resources?

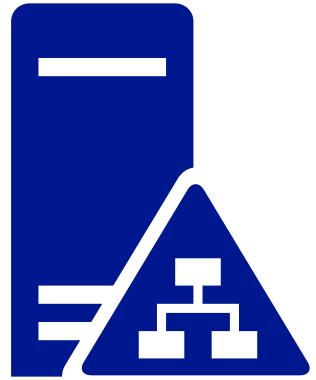
Does each user need the same access level?

Planning for Domain Structure

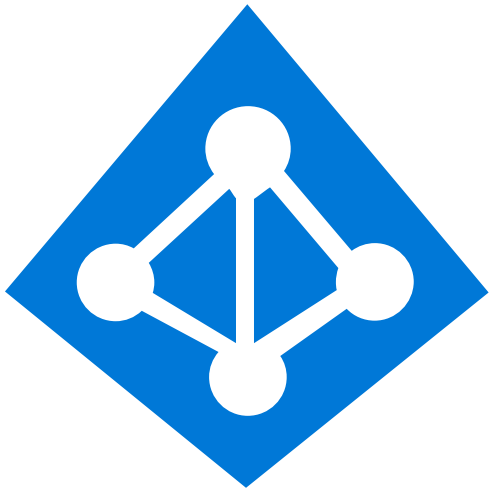


Domain Name

Directory Structure



Federation



Domain Name

What name will your organization use for your domain in the cloud?

Does your organization have a custom domain name?

Is your domain public and easily verifiable via DNS?

Directory Structure

How many AD forests do you have?

How many Azure AD directories?

Will you filter what user accounts are synchronized with the Azure AD?

Do you have multiple Azure AD Connect servers planned?

Do you have a different directory that users authenticate against?

Federation

Will you use the Azure Federation or on-premises AD FS?

More federation services for identities are provided now through Azure

Does your organization use smart cards for Multi Factor Authentication

Restrictions for Connecting Directories

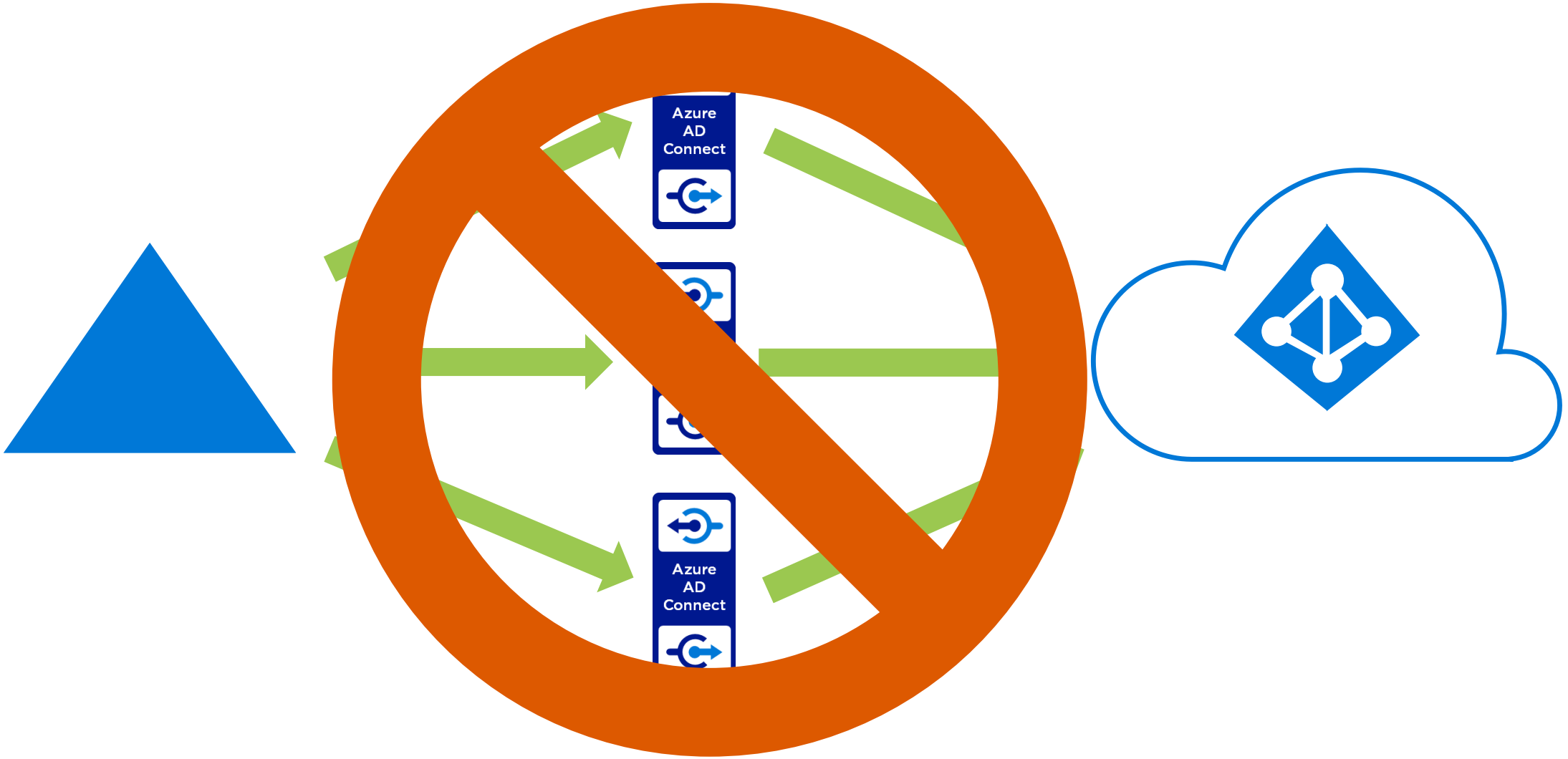
You cannot have multiple Azure AD Connect sync servers connecting to the same Azure AD directory

The same user account cannot sync to multiple Azure AD directories

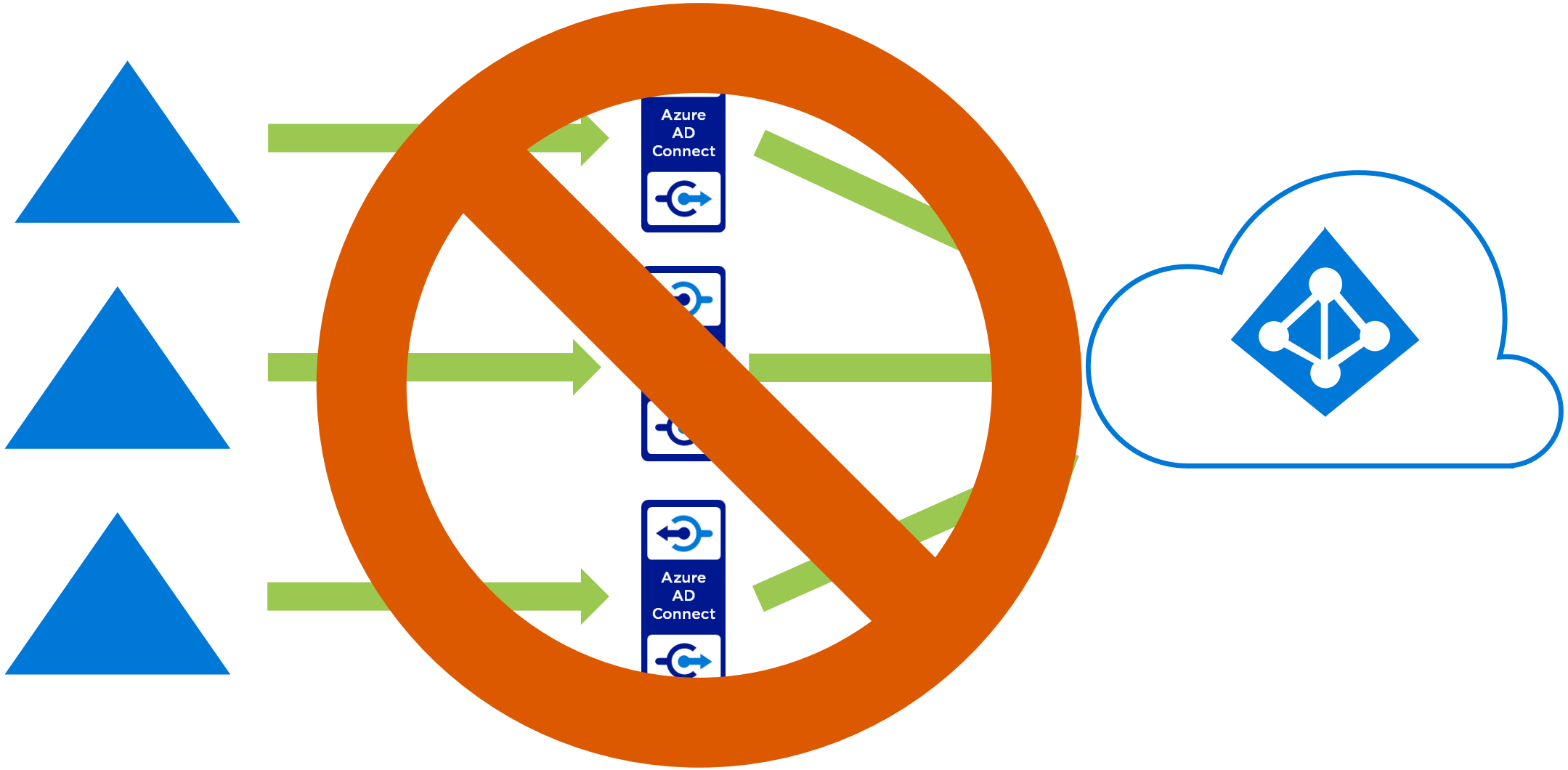
Azure AD Connect cannot connect to multiple Azure AD directories

Users in one Azure AD cannot appear as contacts in another Azure AD directory

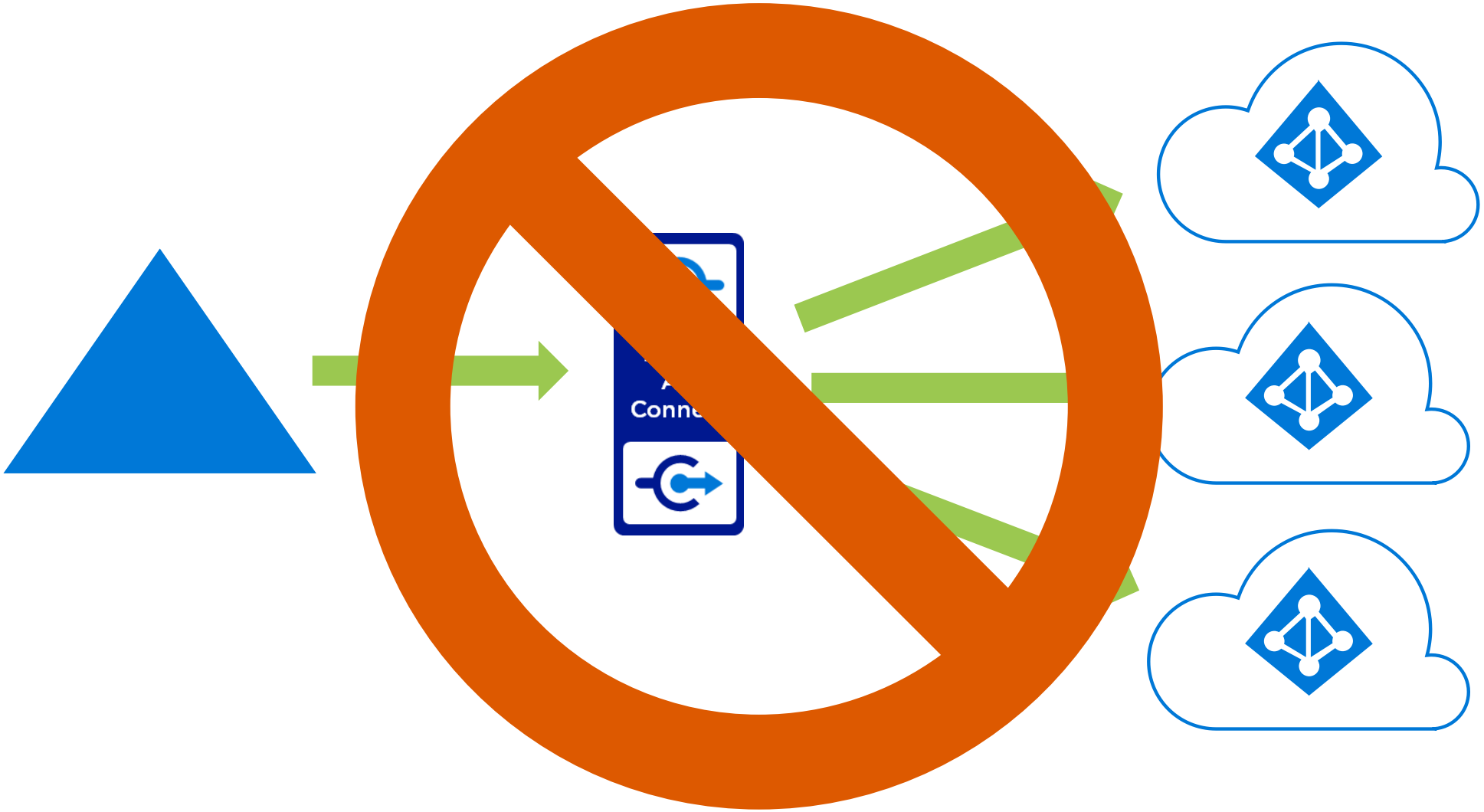
Multiple AAD Connect to Single Azure AD



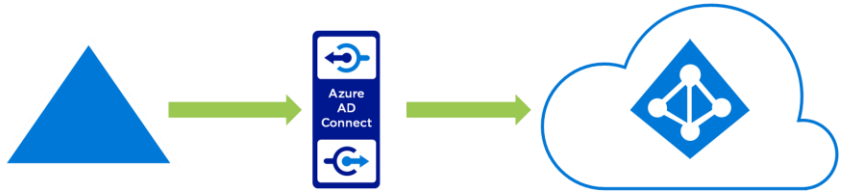
Multiple AAD Connect to Single Azure AD

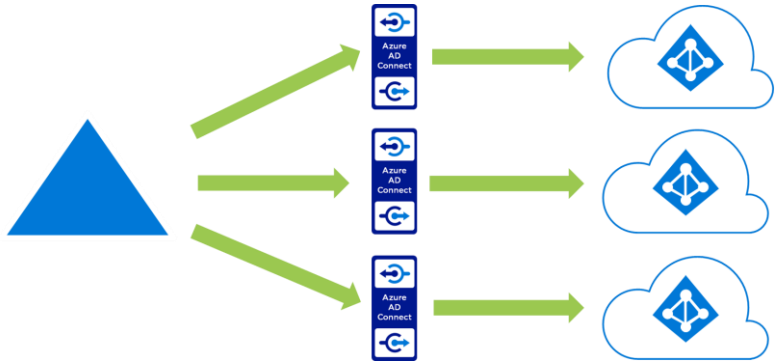


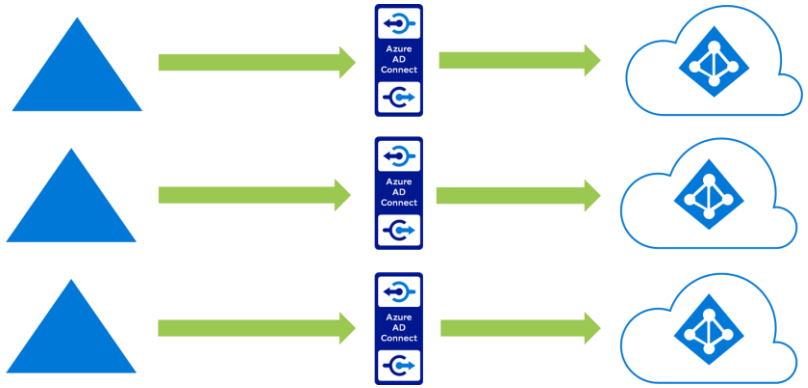
Single AAD Connect to Multi-Azure AD

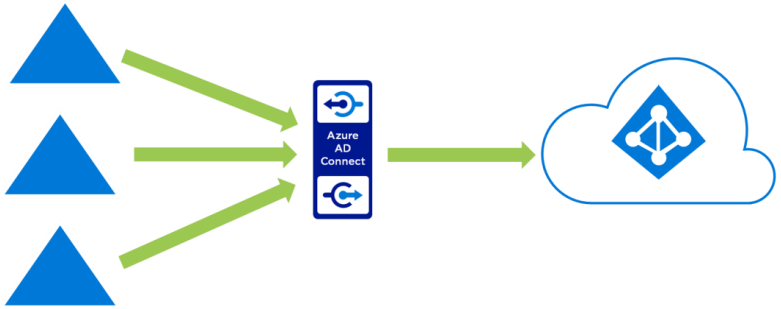


Forest to Azure AD Topology

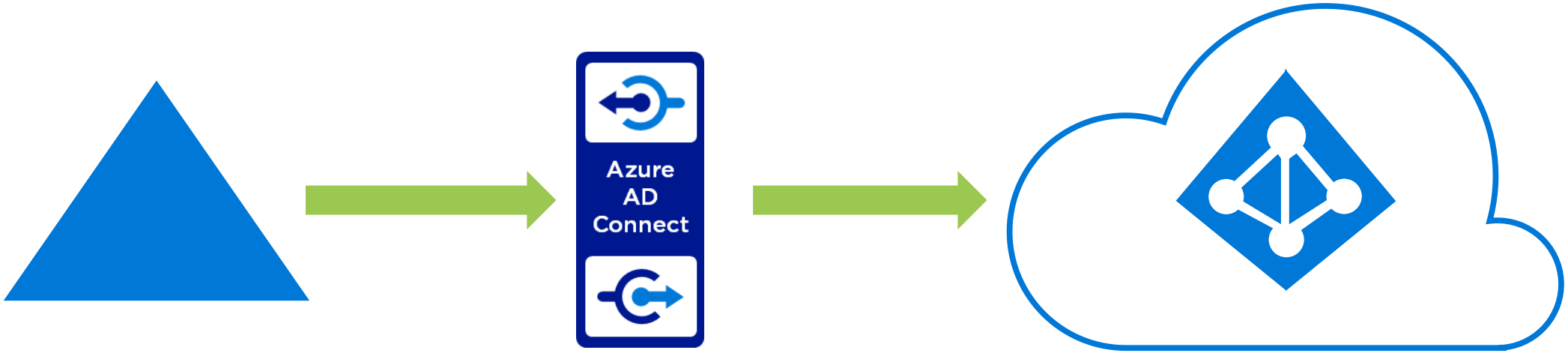








Single Forest to Single Azure AD

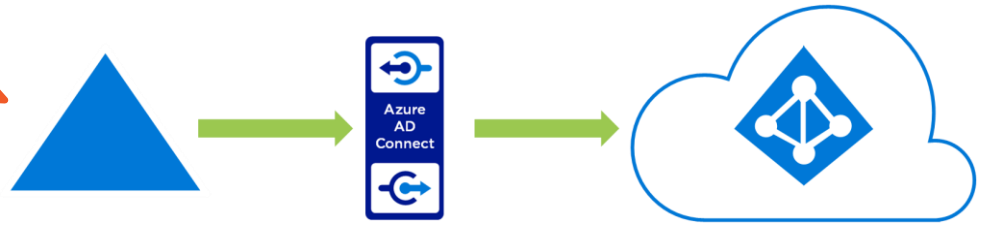


Single Forest to Single Azure AD

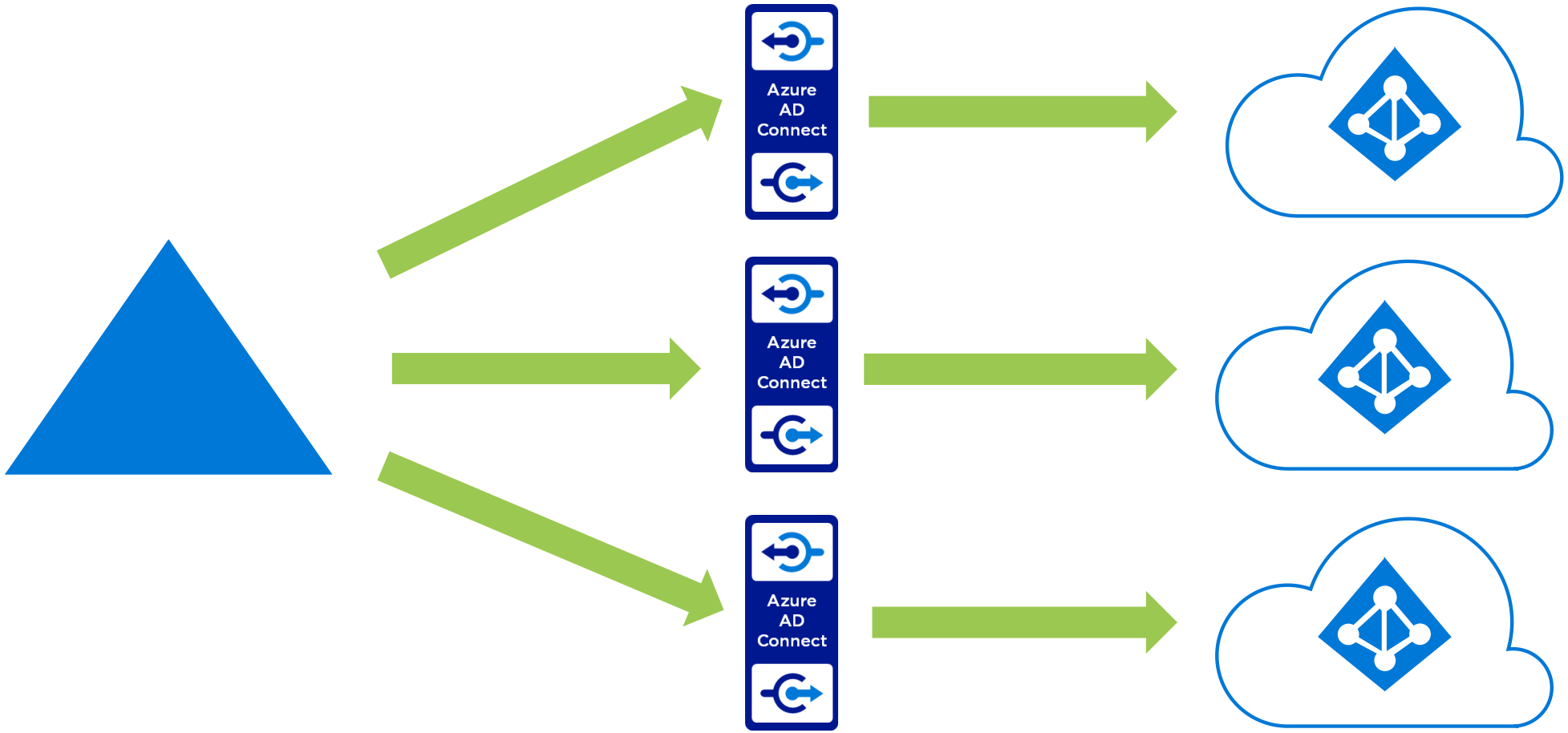
The most common topology

The expected topology when using Azure AD Connect Express installation

Supports multiple domains



Single Forest to Multiple Azure AD



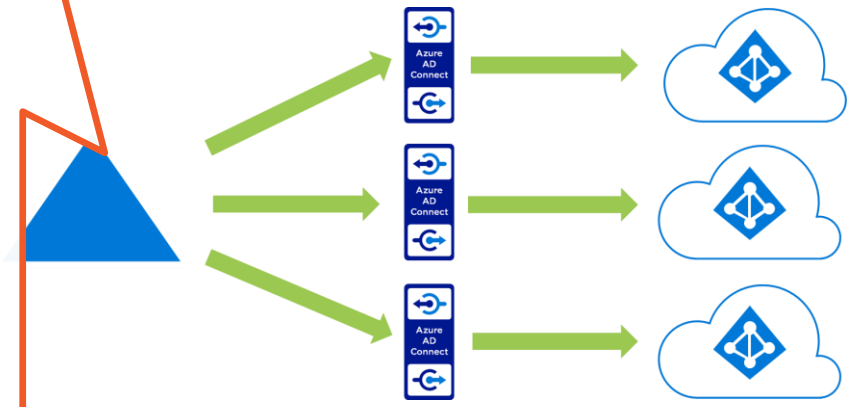
Single Forest to Multiple Azure AD

Azure AD Connect sync servers must be configured for mutually exclusive filtering

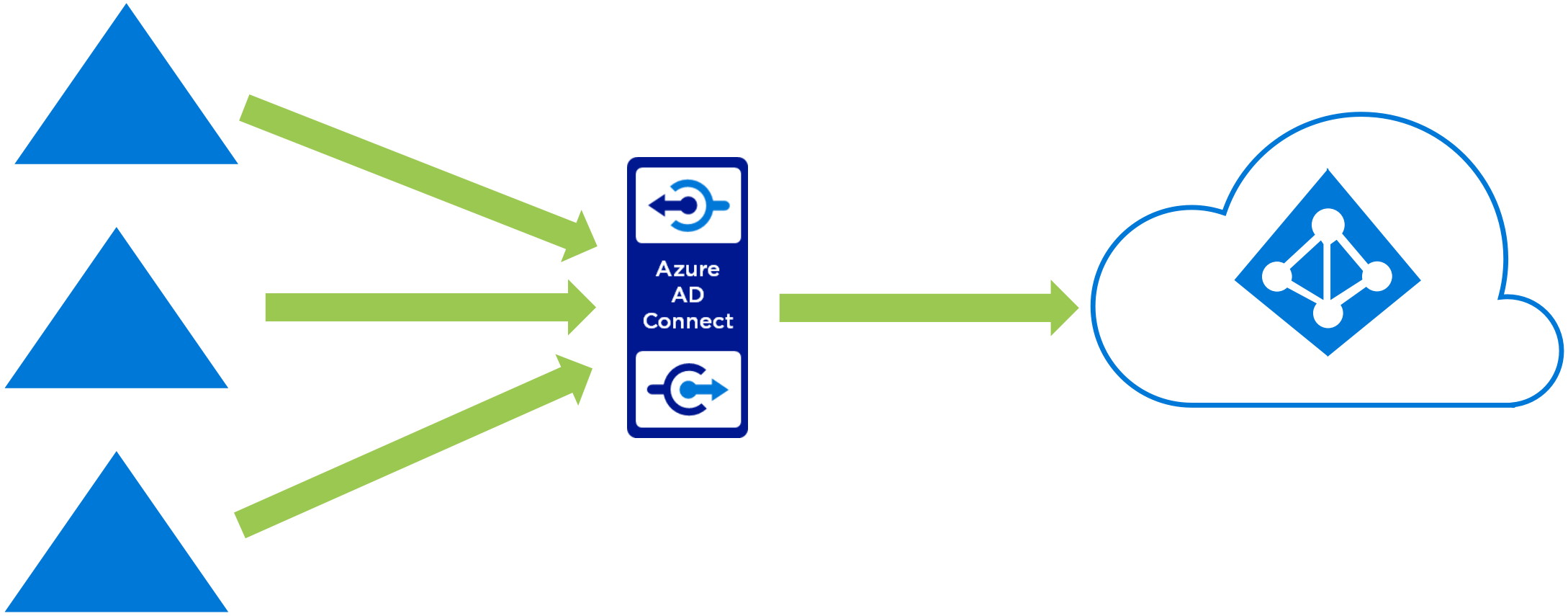
Users in one Azure AD will only be able to see users from their own Azure AD instance

A DNS domain can only be registered in a single Azure AD directory

Some write-back features not supported with this topology



Multiple Forest to Single Azure AD



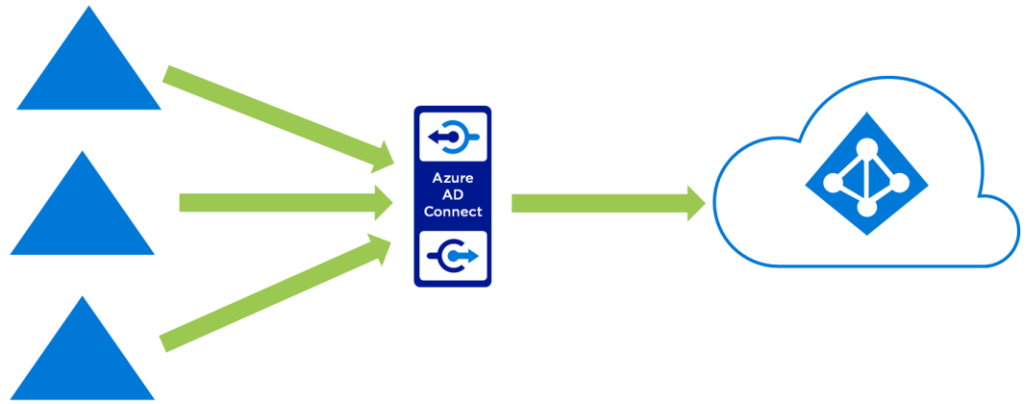
Multiple Forest to Single Azure AD

Users must have only one identity across all forests

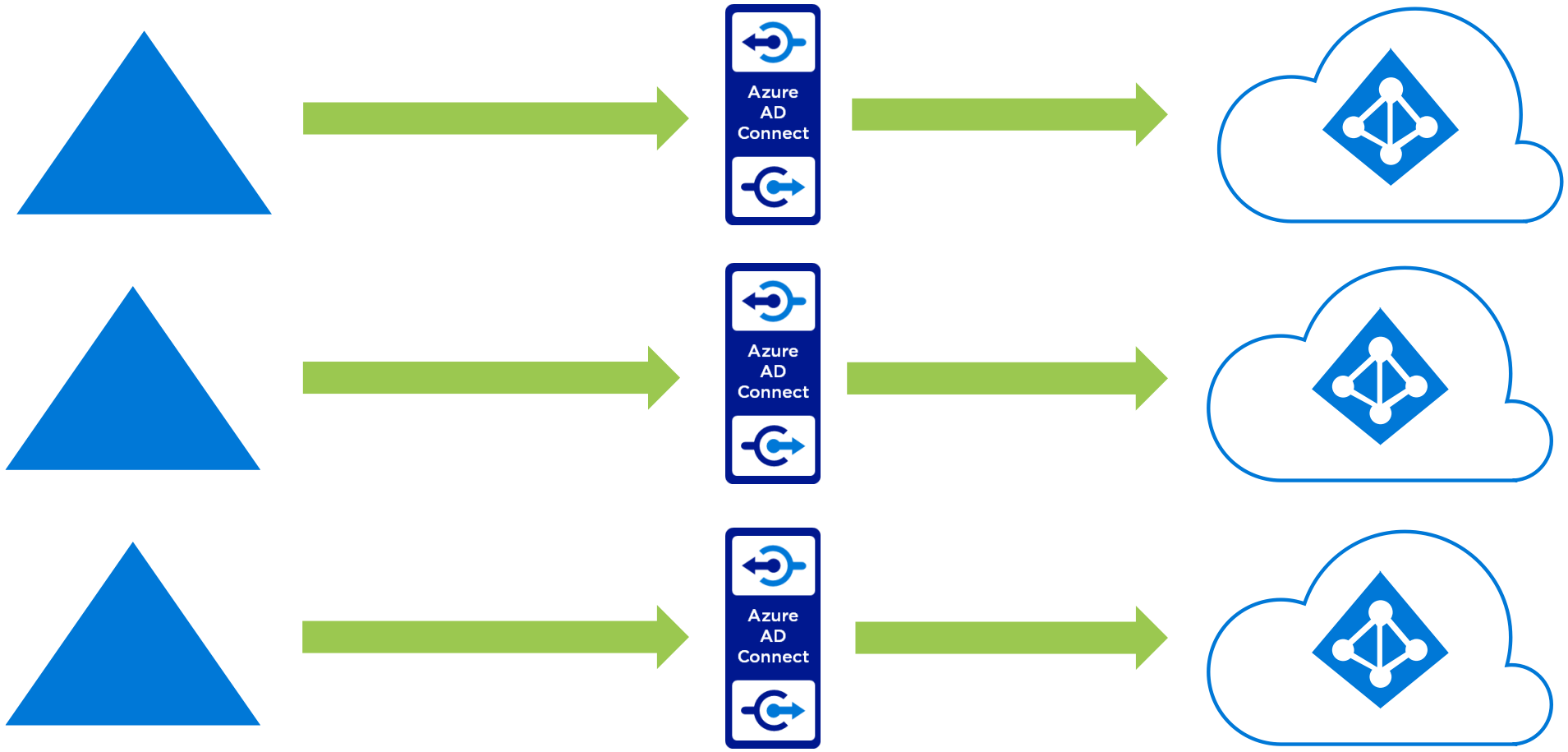
The user authenticates to the forest in which their identity is located

All forests are accessible by Azure AD Connect

Users have only one mailbox



Multiple Forest to Multiple Azure AD



Multiple Forest to Multiple Azure AD

For each instance of Azure AD, you will need an installation of Azure AD Connect

Users in one Azure AD will only be able to see users from their AAD instance

It is recommended to have just a single directory in Azure AD for an organization