Contoso in the Microsoft Cloud

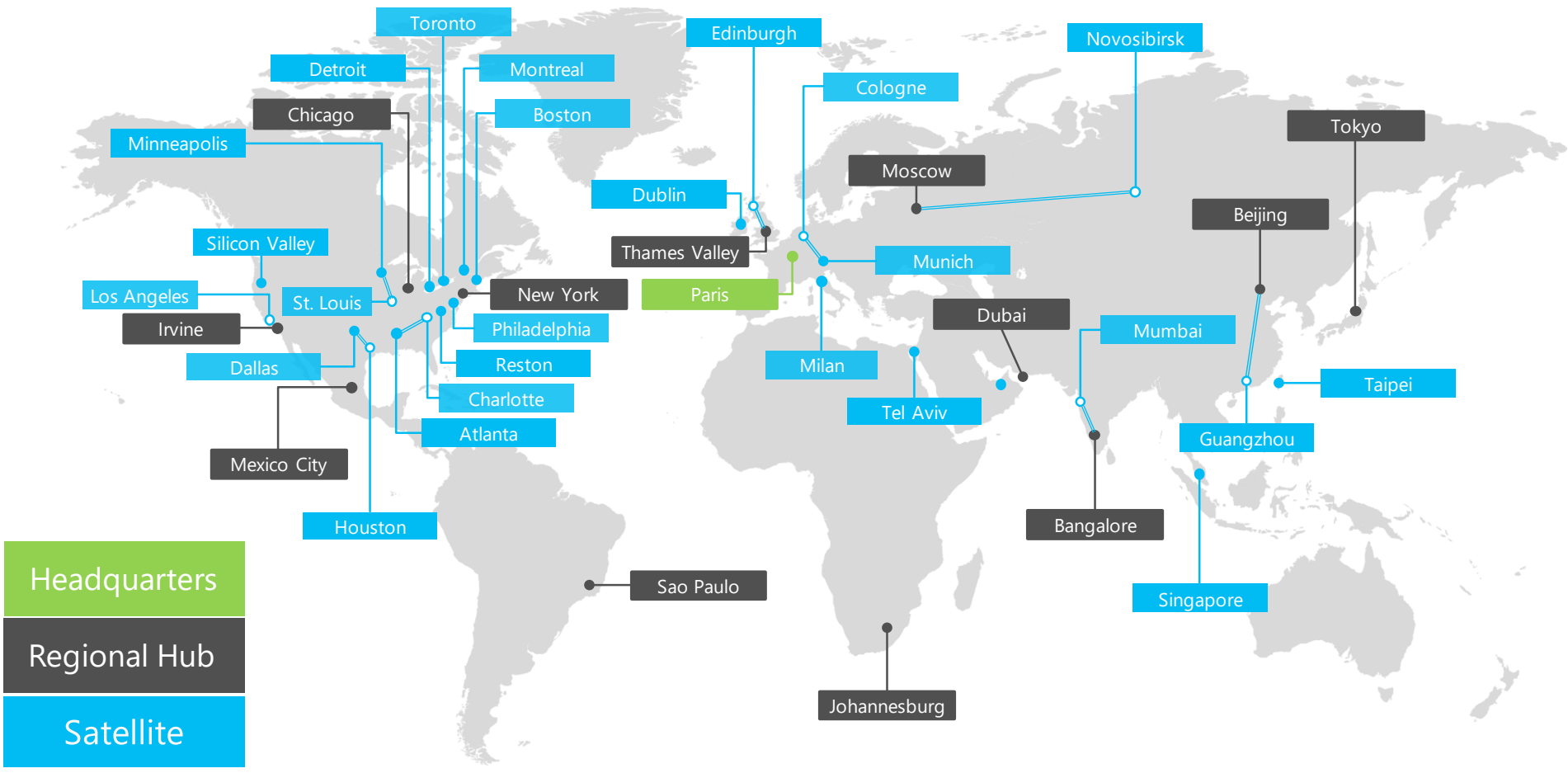
How a fictional but representative global organization has implemented the Microsoft Cloud

This topic is 1 of 6 in a series 1 2 3 4 5 6

The Contoso Corporation

The Contoso Corporation is a global business with headquarters in Paris, France. It is a conglomerate manufacturing, sales, and support organization with over 100,000 products.

Contoso's worldwide organization



Contoso's offices around the world follow a three tier design.

Headquarters

The Contoso Corporation headquarters is a large corporate campus on the outskirts of Paris with dozens of buildings for administrative, engineering, and manufacturing facilities. All of Contoso's datacenters and it's Internet presence are housed in the Paris headquarters.

The headquarters has 15,000 workers.

Regional hubs

Regional hub offices serve a specific region of the world with 60% sales and support staff. Each regional hub is connected to the Paris headquarters with a high-bandwidth WAN link.

Each regional hub has an average of 2,000 workers.

Satellite offices

Satellite offices contain 80% sales and support staff and provide a physical and on-site presence for Contoso customers in key cities or sub-regions. Each satellite office is connected to a regional hub with a high-bandwidth WAN link.

Each satellite office has an average of 250 workers.

25% of Contoso's workforce is mobile-only, with a higher percentage of mobile-only workers in the regional hubs and satellite offices.

Providing better support for mobile-only workers is an important business goal for Contoso.

Elements of Contoso's implementation of the Microsoft cloud

Contoso's IT architects have identified the following elements when planning for the adoption of Microsoft's cloud offerings.

Networking

Networking includes the connectivity to Microsoft's cloud offerings and enough bandwidth to be performant under peak loads. Some connectivity will be over local Internet connections and some will be across Contoso's private network infrastructure.

Microsoft Cloud Networking for Enterprise Architects

Identity

Contoso uses a Windows Server AD forest for its internal identity provider and also federates with third-party providers for customer and partners. Contoso must leverage the internal set of accounts for Microsoft's cloud offerings. Access to cloud-based apps for customers and partners must leverage third-party identity providers as well.

Microsoft Cloud Identity for Enterprise Architects

Security

Security for cloud-based identities and data must include data protection, administrative privilege management, threat awareness, and the implementation of data governance and security policies.

Microsoft Cloud Security for Enterprise Architects

Management

Management for cloud-based apps and SaaS workloads will need the ability to maintain settings, data, accounts, policies, and permissions and to monitor ongoing health and performance. Existing server management tools will be used to manage virtual machines in Azure IaaS.

September 2016

Microsoft

Contoso in the Microsoft Cloud

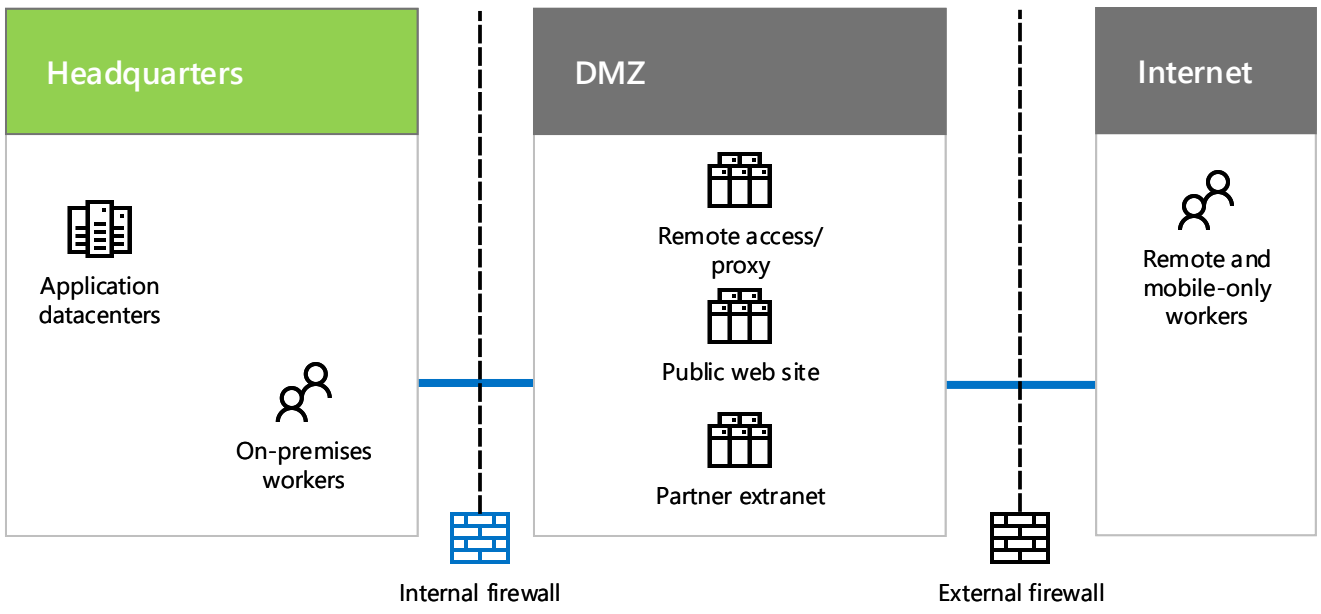
How a fictional but representative global organization has implemented the Microsoft Cloud

Contoso's IT infrastructure and needs

Contoso is in the process of transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive one that incorporates cloud-based personal productivity workloads, applications, and hybrid scenarios.

Contoso's existing IT infrastructure

Contoso uses a mostly centralized on-premises IT infrastructure, with application datacenters in the Paris headquarters.



In Contoso's DMZ, different sets of servers provide:

- Remote access to the Contoso intranet and web proxying for workers in the Paris headquarters.
- Hosting for the Contoso public web site, from which customers can order products, parts, or supplies.
- Hosting for the Contoso partner extranet for partner communication and collaboration.

Contoso's business needs

1 Adhere to regional regulatory requirements

To prevent fines and maintain good relations with local governments, Contoso must ensure compliance with data storage and encryption regulations.

2 Improve vendor and partner management

The partner extranet is aging and expensive to maintain. Contoso wants to replace it with a cloud-based solution that uses federated authentication.

3 Improve mobile workforce productivity, device management, and access

Contoso's mobile-only workforce is expanding and needs device management to ensure intellectual property protection and more efficient access to resources.

4 Reduce remote access infrastructure

By moving resources commonly accessed by remote workers to the cloud, Contoso will save money by reducing maintenance and support costs for their remote access solution.

5 Scale down on-premises datacenters

The Contoso datacenters contain hundreds of servers, some of which are running legacy or archival functions that distract IT staff from maintaining high business value workloads.

6 Scale-up computing and storage resources for end-of-quarter processing

End-of-quarter financial accounting and projection processing along with inventory management requires short-term increases in servers and storage.

Mapping Contoso's business needs to Microsoft's cloud offerings

SaaS
Software as a Service

- **Office 365:** Primary personal and group productivity applications in the cloud. (1, 3, 5)
- **Dynamics 365:** Use cloud-based customer and vendor management. Remove partner extranet in the DMZ. (2)
- **Intune/EMS:** Manage iOS and Android devices. (3)

Azure PaaS
Platform as a Service

- Host sales and support documents and information systems using cloud-based apps. (3)
- Mobile applications are cloud-based, rather than Paris datacenter-based. (3, 4)

Azure IaaS
Infrastructure as a Service

- Move archival and legacy systems to cloud-based servers. (5)
- Migrate low-use apps and data out of on-premises datacenters. (5)
- Add temporary servers and storage for end-of-quarter processing needs. (6)

September 2016

Microsoft

Contoso in the Microsoft Cloud

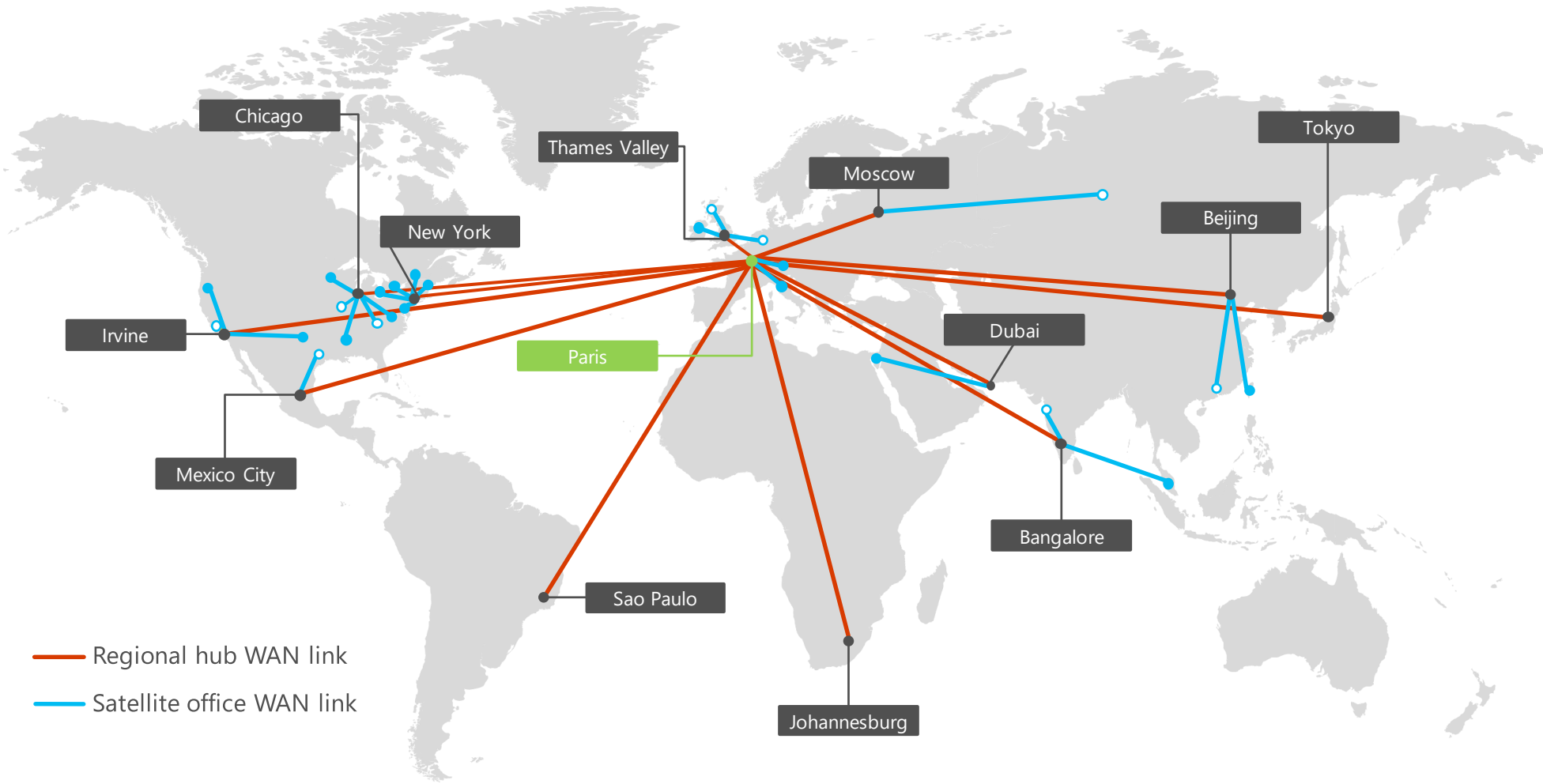
How a fictional but representative global organization has implemented the Microsoft Cloud

Networking

To adopt a cloud-inclusive infrastructure, Contoso's network engineers realized the fundamental shift in the way that network traffic to cloud-based services travels. Instead of only optimizing traffic to on-premises servers and datacenters, equal attention must be paid to optimizing traffic to the Internet edge and across the Internet.

Contoso's networking infrastructure

Contoso has the following networking infrastructure.



On-premises network

WAN links connect the Paris headquarters to regional offices and regional offices to satellite offices in a spoke and hub configuration.

Within each office, routers deliver traffic to hosts or wireless access points on subnets, which use the private IP address space.

Internet connectivity

Each office has its own Internet connectivity via a proxy server.

This is typically implemented as a WAN link to a local ISP that also provides public IP addresses for the proxy server.

Internet presence

Contoso owns the contoso.com public domain name.

The Contoso public web site for ordering products is a set of servers in an Internet-connected datacenter in the Paris campus.

Contoso uses a /24 public IP address range on the Internet.

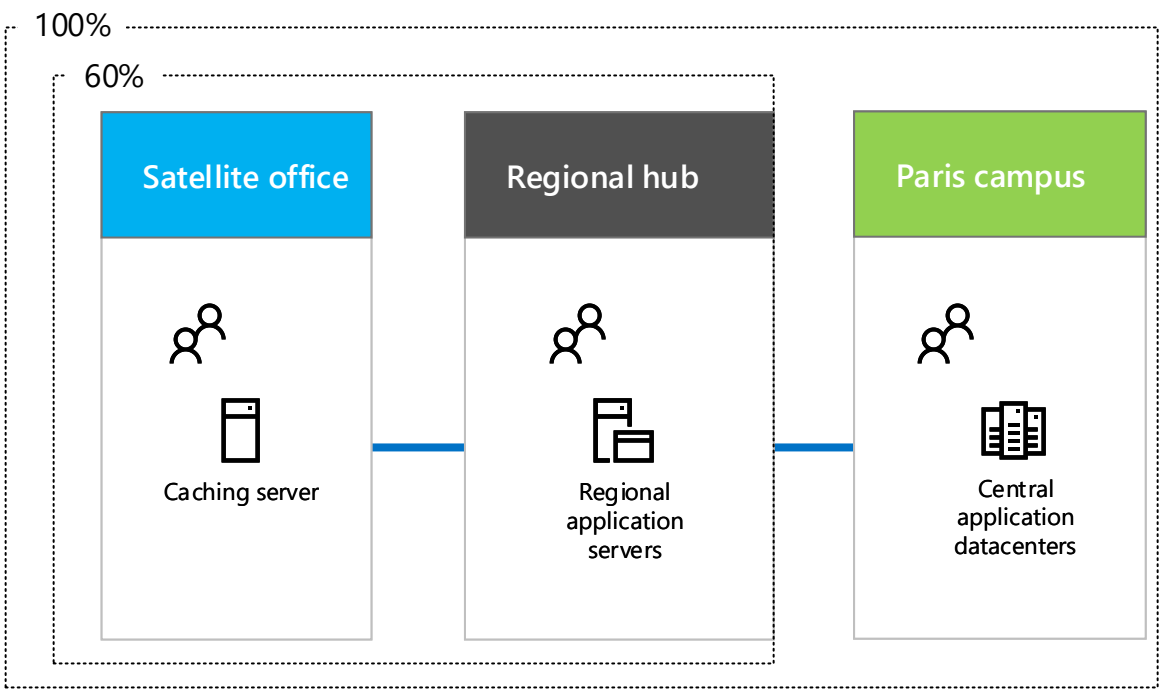
Contoso's app infrastructure

Contoso has architected its application and server infrastructure for the following:

- Satellite offices use local caching servers to store frequently-accessed documents and internal web sites.
- Regional hubs use regional application servers for the regional and satellite offices. These servers synchronize with servers in the Paris headquarters.
- The Paris campus has the datacenters that contain the centralized application servers that serve the entire organization.

For users in satellite or regional hub offices, 60% of the resources needed by employees can be served by satellite and regional hub office servers. The additional 40% of resource requests must go over the WAN link to the Paris campus.

Continued on next page



Contoso's network analysis

Here are the results of Contoso's analysis of the changes needed on their network to accommodate the different categories of Microsoft's cloud offerings.

SaaS cloud offerings
Office 365, EMS, and Dynamics 365

Successful adoption of SaaS services by users depends on highly-available and performant connectivity to the Internet, or directly to Microsoft cloud services.

For mobile users, their current Internet access is assumed to be adequate.

For users on the Contoso intranet, each office must be analyzed and optimized for throughput to the Internet and round-trip times to Microsoft's Europe datacenter hosting the Office 365, EMS, and Dynamics 365 tenants.

Azure PaaS
Mobile applications

To better support mobile workers, legacy apps and some file sharing sites are being reworked and deployed as Azure PaaS apps. For optimum performance, Contoso plans to deploy the new apps from multiple Azure datacenters across the world. Azure Traffic Manager to send client app requests, whether they originate from a mobile user or a computer in the office, to the nearest Azure datacenter hosting the app.

The IT department will need to add PaaS application performance and traffic distribution to their network health monitoring solution.

Azure IaaS
Server-based workloads

To move some legacy and archival servers out of the Paris campus datacenters and add servers as needed for quarter-end processing, Contoso plans to use virtual machines running in Azure infrastructure services.

The Azure virtual networks that contain these servers must be designed for non-overlapping address spaces, routing, and integrated DNS.

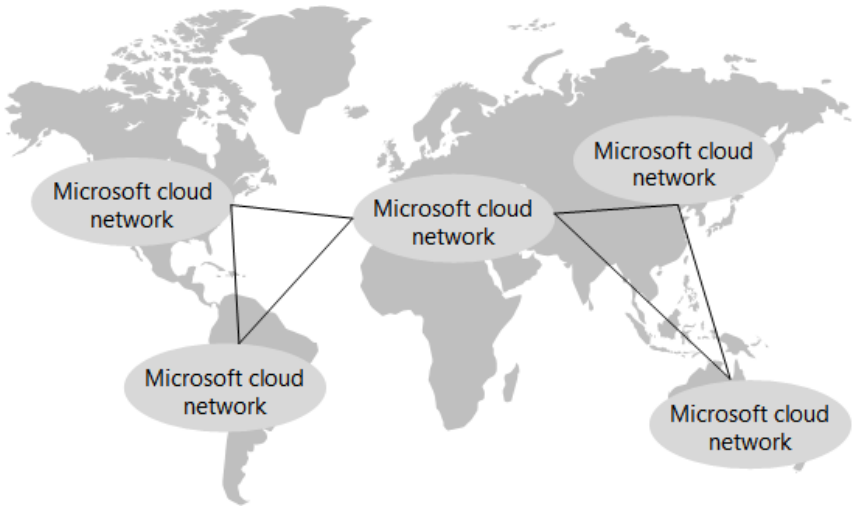
The IT department must include these new servers in their network management and monitoring system.

Contoso's use of ExpressRoute

ExpressRoute is a dedicated WAN connection from your location to a Microsoft peering location that connects your network to the Microsoft cloud network. ExpressRoute connections provide predictable performance and a 99.9% uptime SLA.

With an ExpressRoute connection, you are connected to the Microsoft cloud network and all the Microsoft datacenter locations in the same continent. The traffic between the cloud peering location and the destination Microsoft datacenter is carried over the Microsoft cloud network.

With ExpressRoute Premium, you can reach any Microsoft datacenter on any continent from any Microsoft peering location on any continent. The traffic between continents is carried over the Microsoft cloud network.



Based on the analysis of current and future traffic to Microsoft's cloud offerings and its requirements for high quality of service for Skype-based communications, Contoso has performed a network assessment and implemented an any-to-any (MPLS-based) ExpressRoute Premium connection from the Paris headquarters to the Microsoft peering location in Europe.

Consistent performance for Paris campus staff for SaaS applications

With 15,000 employees in the Paris campus all simultaneously accessing Office 365, Intune, and Dynamics 365, Contoso wants to ensure that that access is consistently performant and is not competing with regional Internet traffic.

Consistent performance for administration of distributed Azure PaaS apps

All of Contoso's application developers and core infrastructure IT administrators are in the Paris campus.

With Azure PaaS apps distributed to different Azure datacenters around the world, Contoso needs consistent performance from the Paris campus to administer the apps and their storage resources, which consist of TB of documents.

Consistent performance for administration of servers in Azure IaaS

Contoso's datacenter administrators are in the Paris campus and the servers to be deployed in Azure are an extension of the Paris datacenter.

Contoso needs consistent performance to these new servers for access to legacy apps and archival storage and for end-of-quarter processing.

Contoso's path to cloud networking readiness

1. **Optimize employee computers for Internet access**
   Individual computers will be checked to ensure that the latest TCP/IP stack, browser, NIC drivers, and security and operating system updates are installed.
2. **Analyze Internet connection utilization at each office and increase as needed**
   Each office will be analyzed for the current Internet usage and WAN link bandwidth will be increased if operating at 70% or above utilization.
3. **Analyze DMZ systems at each office for optimal performance**
   Firewalls, IDSs, and other systems in the Internet path will be analyzed for optimal performance. Proxy servers will be updated or upgraded as needed.
4. **Add ExpressRoute Premium for the Paris campus**
   Provides consistent access to SaaS cloud offerings for Paris campus workers and administration of Azure PaaS and IaaS workloads across the world.
5. **Create and test an Azure Traffic Manager profile for Azure PaaS apps**
   Test an Azure Traffic Manager profile that uses the performance routing method to gain experience in distributing Internet traffic to regional locations.
6. **Reserve private address space for Azure VNets**
   Based on the numbers of projected short and long-term servers in Azure IaaS, reserve private address space for Azure VNets and their subnets.

Cloud networking resources

Microsoft Cloud Networking for Enterprise Architects
http://aka.ms/cloudarchnetworking

Network planning and performance tuning for Office 365
http://aka.ms/tune

ExpressRoute for Office 365
http://aka.ms/expressrouteoffice365

September 2016

Microsoft

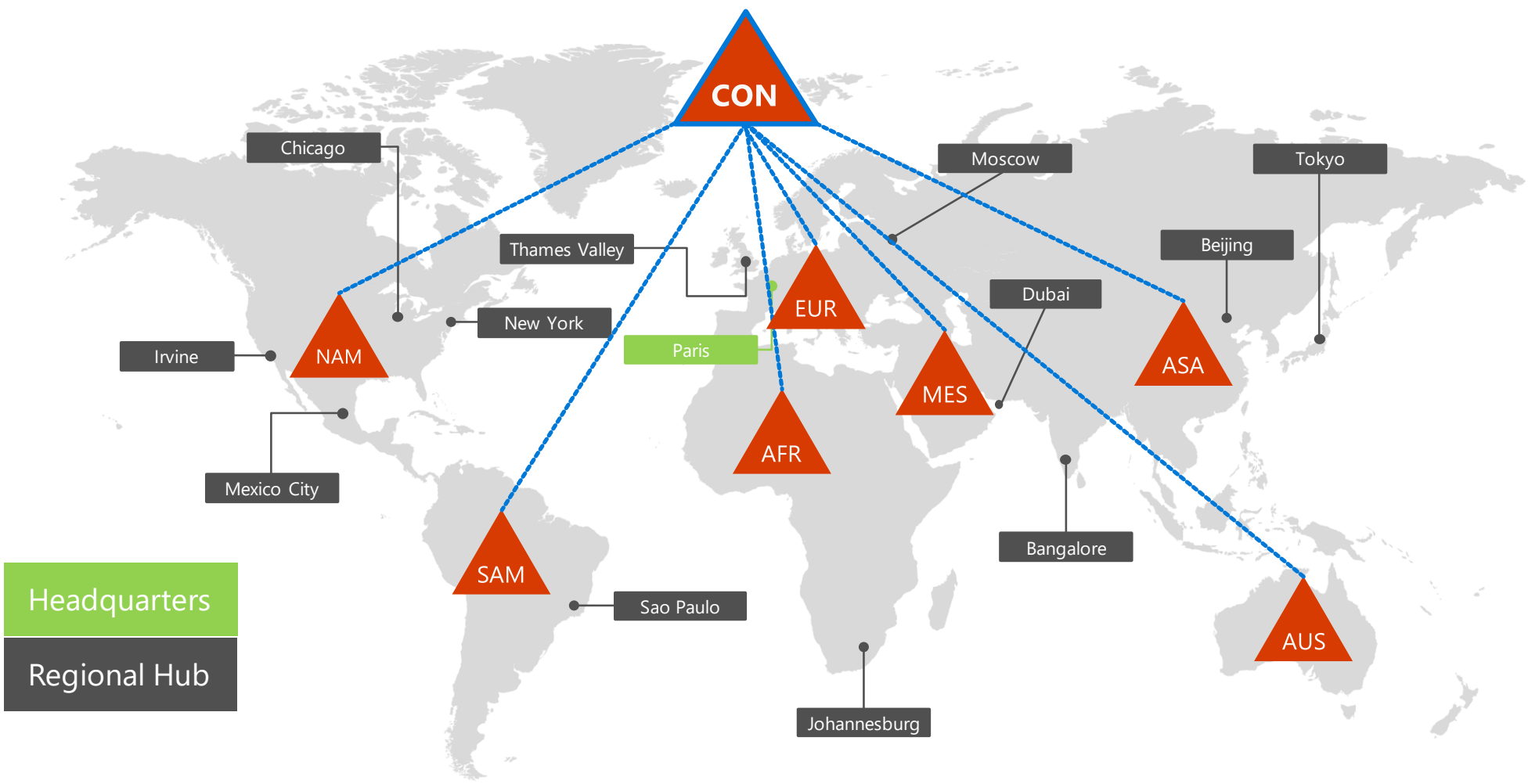
Contoso in the Microsoft Cloud

How a fictional but representative global organization has implemented the Microsoft Cloud

Identity

Microsoft provides an Identity as a Service (IDaaS) across its cloud offerings. To adopt a cloud-inclusive infrastructure, Contoso's IDaaS solution must leverage their on-premises identity provider and include federated authentication with their existing trusted, third-party identity providers.

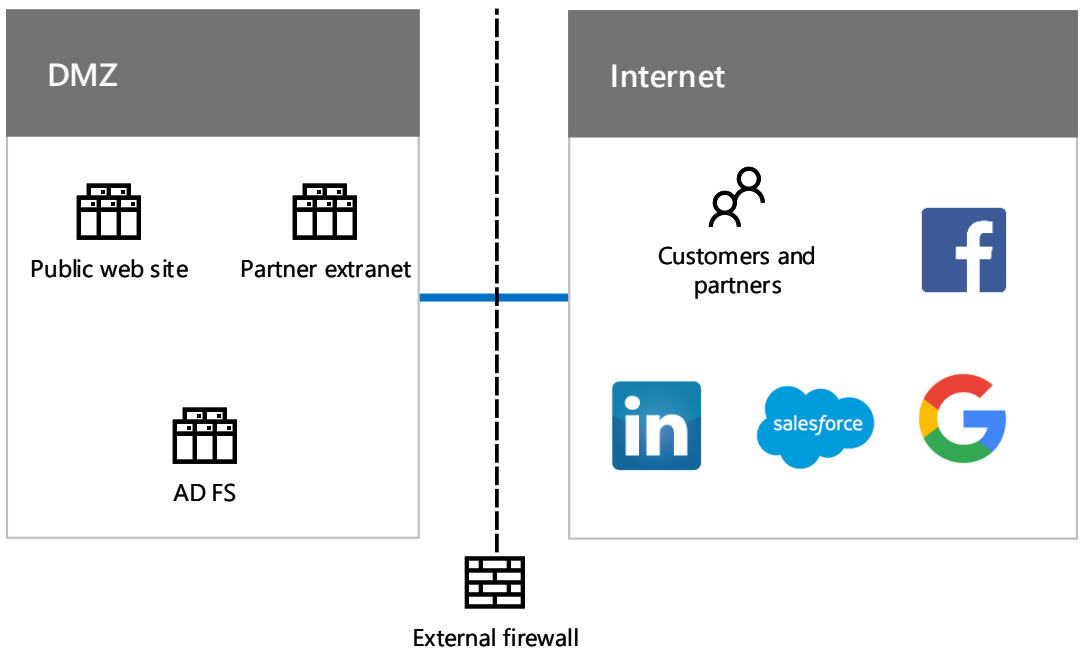
Contoso's Windows Server AD forest



Contoso uses a single Windows Server Active Directory (AD) forest for contoso.com with seven domains, one for each region of the world. The headquarters, regional hub offices, and satellite offices contain domain controllers for local authentication and authorization.

Contoso wants to use the accounts and groups in the contoso.com forest for authentication and authorization for its cloud-based apps and workloads.

Contoso's federated authentication infrastructure



Contoso allows:

- Customers to use their Microsoft, Facebook, or Google Mail accounts to sign in to their public web site.
- Vendors and partners to use their LinkedIn, Salesforce, or Google Mail accounts to sign in to the partner extranet.

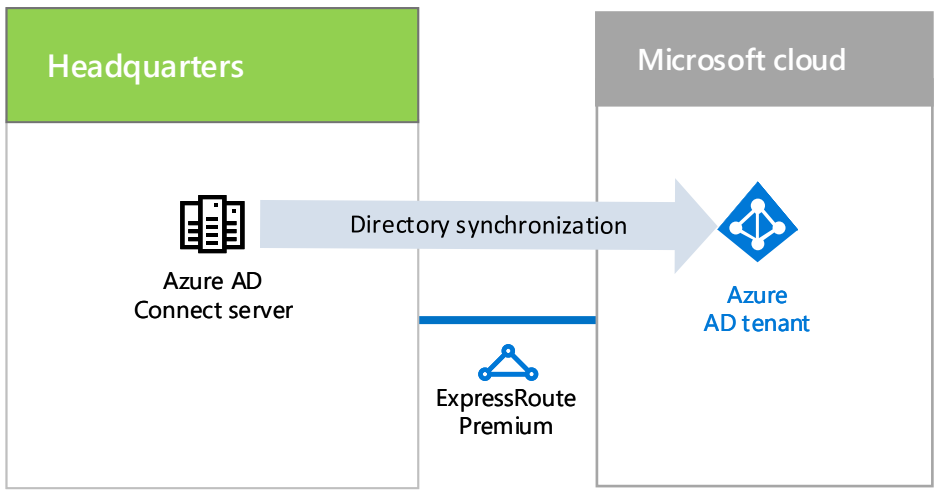
Active Directory Federation Services (AD FS) servers in the DMZ authenticate customer credentials for access to the public web site and partner credentials for access to the partner extranet.

When Contoso transitions its public web site to an Azure Web App and partner extranet to Dynamics 365, they want to continue to use these third-party identity providers for their customers and partners.

This will be accomplished by configuring federation between Contoso Azure AD tenants and these third-party identity providers.

Continued on next page

Directory synchronization for Contoso's Windows Server AD forest



Contoso has deployed the Azure AD Connect tool on a cluster of servers in its Paris datacenter. Azure AD Connect synchronizes changes to the contoso.com Windows Server AD forest with the Azure AD tenant shared by Contoso's Office 365, EMS, Dynamics 365, and Azure subscriptions. For more information about subscriptions, licenses, user accounts, and tenants, see topic 5.

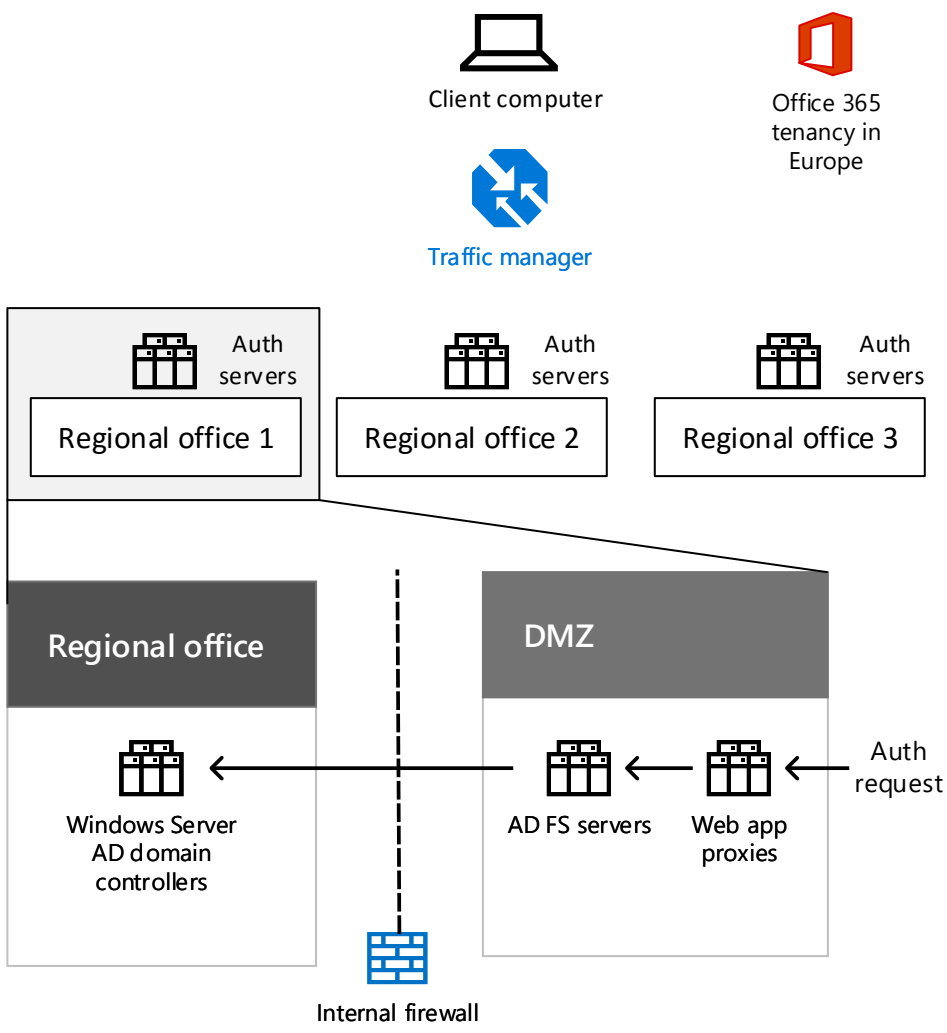
Contoso has configured federated authentication, which provides single sign-on for Contoso's workers. When a user that has already signed in to the contoso.com Windows Server AD forest accesses a Microsoft SaaS or PaaS cloud resource, they will not be prompted for a password.

The traffic for the directory synchronization travels over the ExpressRoute Premium connection from the headquarters campus to the Microsoft cloud network.

Geographical distribution of Contoso authentication traffic

To better support its mobile and remote workforce, Contoso has deployed sets of authentication servers in its regional offices. This infrastructure distributes the load and provides redundancy and higher performance when authenticating user credentials for access to Microsoft cloud offerings that use the common Azure AD tenant.

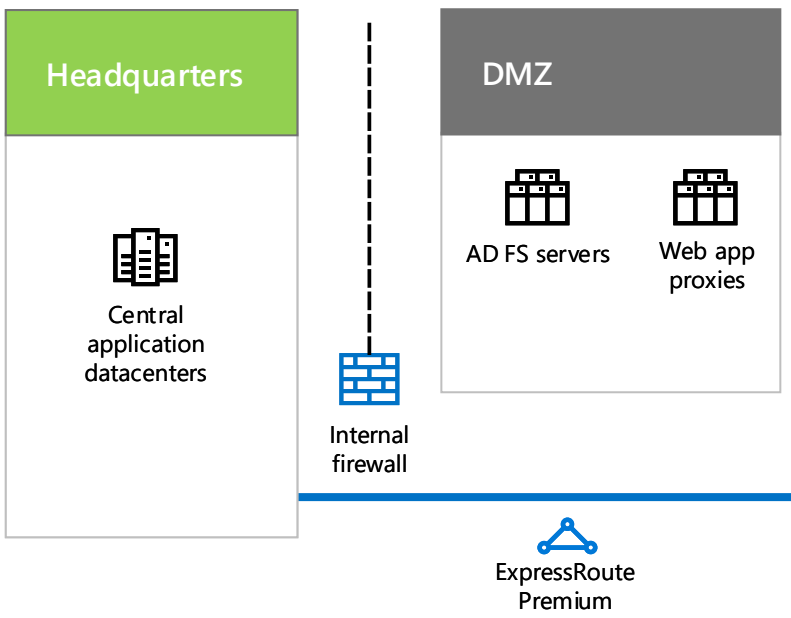
To distribute the load of authentication requests, Contoso has configured Azure Traffic Manager with a profile that uses the performance routing method, which refers authenticating clients to the regionally closest set of authentication servers.



Authentication process example:

1. The client computer initiates communication with a web page in the Office 365 tenancy in Europe (such as sharepoint.contoso.com).
2. Office 365 sends back a request to send proof of authentication. The request contains the URL to contact for authentication.
3. The client computer attempts to resolve the DNS name in the URL to an IP address.
4. Azure Traffic Manager receives the DNS query and responds to the client computer with the IP address of a web application proxy server in the regional office that is closest to the client computer.
5. The client computer sends an authentication request to a web application proxy server, which forwards the request to an AD FS server.
6. The AD FS server requests the user credentials from the client computer.
7. The client computer sends the user credentials without prompting the user.
8. The AD FS server validates the credentials with a Windows Server AD domain controller in the regional office and returns a security token to the client computer.
9. The client computer sends the security token to Office 365.
10. After successful validation, Office 365 caches the security token and sends the web page requested in step 1 to the client computer.

Redundancy for the headquarters authentication infrastructure in Azure IaaS



To provide redundancy for the remote and mobile workers of the Paris headquarters that contains 15,000 workers, Contoso has deployed a second set of application proxies and AD FS servers in Azure IaaS.

When the primary authentication servers in the headquarters DMZ become unavailable, IT staff switch over to the redundant set deployed in Azure IaaS. Subsequent authentication requests from Paris office computers use the set in Azure IaaS until the availability problem is corrected.

To switch over and switch back, Contoso updates the Azure Traffic Manager profile for the Paris region to use a different set of IP addresses for the web application proxies:

- When the DMZ authentication servers are available, use the IP addresses of the servers in the DMZ.
- When the DMZ authentication servers are not available, use the IP addresses of the servers in Azure IaaS.

Cloud identity resources

Microsoft Cloud Identity for Enterprise Architects
http://aka.ms/cloudarchidentity

Infographic: Cloud identity and access management
http://go.microsoft.com/fwlink/p/?LinkId=524282

Synchronizing your directory with Office 365 is easy
http://go.microsoft.com/fwlink/p/?LinkId=524281

September 2016

Microsoft

Contoso in the Microsoft Cloud

How a fictional but representative global organization has implemented the Microsoft Cloud

Subscriptions, licenses, and user accounts

To provide a consistent use of identities and billing for all cloud offerings, Microsoft provides an organization/subscriptions/licenses/user accounts hierarchy.

Organization

The business entity that is using Microsoft cloud offerings, typically identified by a public DNS domain name, such as contoso.com.

Subscriptions

For Microsoft SaaS cloud offerings (Office 365, Intune/EMS, and Dynamics 365), a subscription is a specific product and a purchased set of user licenses.

For Azure, a subscription allows for billing of consumed cloud services to the organization.

Licenses

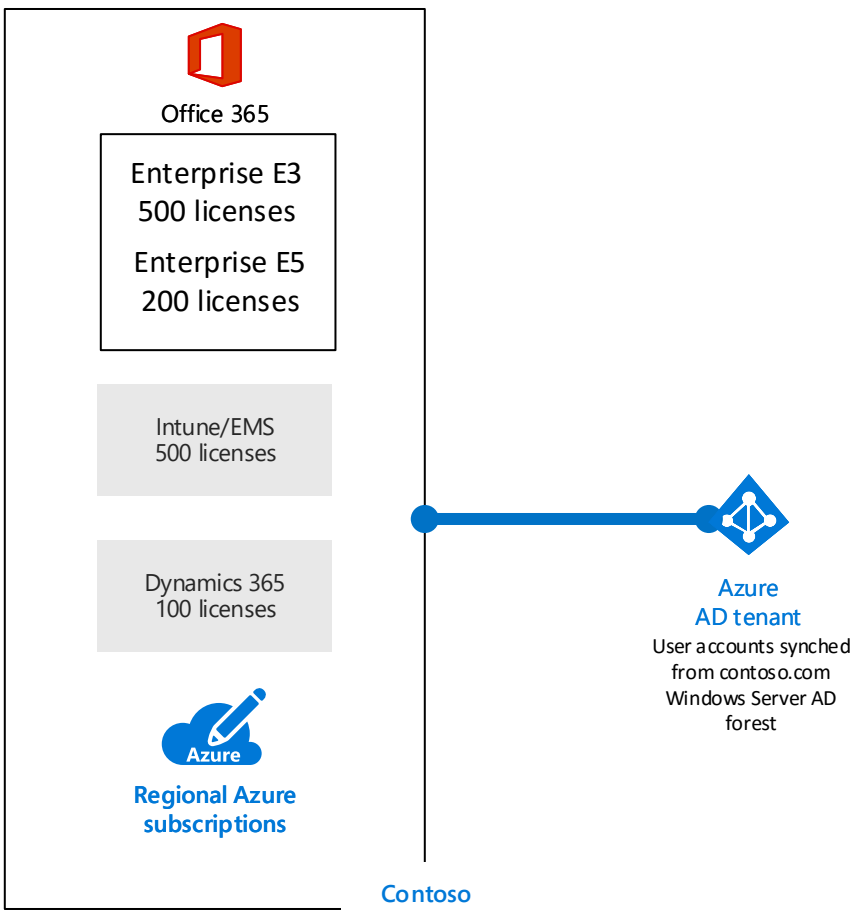
For Microsoft SaaS cloud offerings, a license allows a specific user account to use cloud services.

For Azure, software licenses are built into service pricing, but in some cases you will need to purchase additional software licenses.

User accounts

User accounts are stored in an Azure AD tenant and can be synchronized from an on-premises identity provider such as Windows Server AD.

Contoso's structure



Organization The Contoso Corporation is identified by its public domain name contoso.com.

Subscriptions and licenses The Contoso Corporation is using the following:

- The Office 365 Enterprise E3 product with 500 licenses
- The Office 365 Enterprise E5 product with 200 licenses
- The EMS product with 500 licenses
- The Dynamics 365 product with 100 licenses
- Multiple Azure subscriptions based on regions

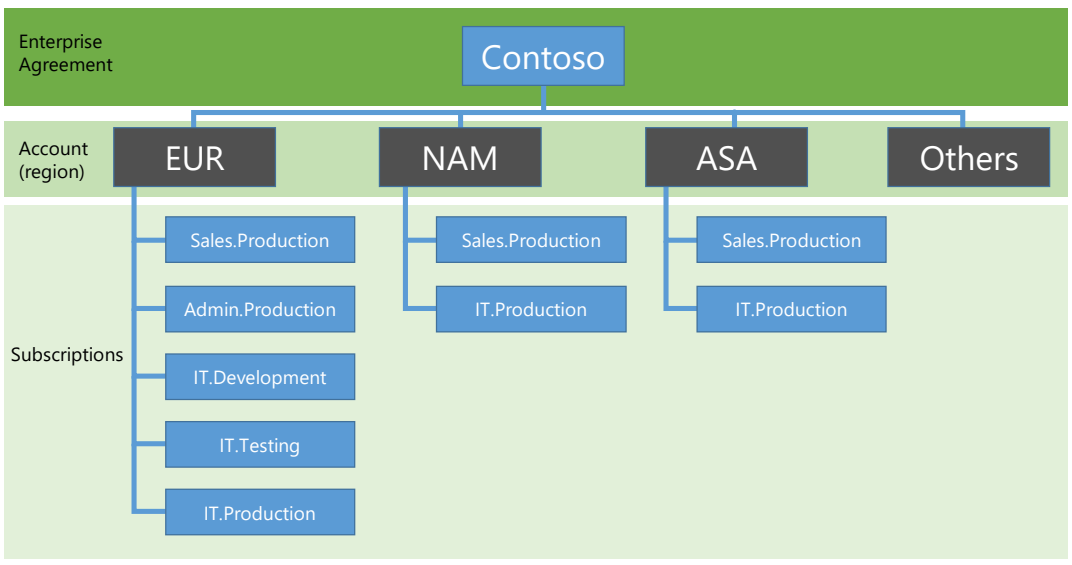
User accounts A common Azure AD tenant contains the list of user accounts and groups used by all of Contoso's subscriptions, with the exception of dev/test Azure subscriptions.

Tenants:

- For SaaS cloud offerings, the tenant is the regional location that houses the servers providing cloud services. Contoso chose the European region to host its Office 365, EMS, and Dynamics 365 tenants.
- Azure PaaS services and apps and IaaS IT workloads can have tenancy in any Azure datacenter across the world.
- An Azure AD tenant is a specific instance of Azure AD containing accounts and groups. The common Azure AD tenant that contains the synchronized accounts for the Contoso Windows Server AD forest provides IDaaS across Microsoft's cloud offerings.

Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings

Contoso's Azure subscriptions



Contoso has designed the following hierarchy for their Azure subscriptions:

- Contoso is at the top, based on its Enterprise Agreement with Microsoft.
- There are a set of accounts corresponding to the different regions of the Contoso Corporation around the world, based on the domains of Contoso's Windows Server AD forest.
- Within each region, there are one or more subscriptions based on the region's development, testing, and production deployment needs.

Each Azure subscription can be associated with a single Azure AD tenant that contains user accounts and groups for authentication and authorization to Azure services. Production subscriptions use the common Contoso Azure AD tenant.

Azure subscription and accounts guidelines

Contoso in the Microsoft Cloud

How a fictional but representative global organization has implemented the Microsoft Cloud

Security

Contoso is serious about their information security and protection. When transitioning their IT infrastructure to a cloud-inclusive one, they made sure that their on-premises security requirements were supported and implemented in Microsoft's cloud offerings.

Contoso's security requirements in the cloud

Strong authentication to cloud resources	Cloud resource access must be authenticated and, where possible, leverage multi-factor authentication.
Encryption for traffic across the Internet	No data sent across the Internet is in plain text form. Always use HTTPS connections, IPsec, or other end-to-end data encryption methods.
Encryption for data at rest in the cloud	All data stored on disks or elsewhere in the cloud must be in an encrypted form.
ACLs for least privilege access	Account permissions to access resources in the cloud and what they are allowed to do must follow least-privilege guidelines.

Contoso's data sensitivity classification

Using the information in Microsoft's Data Classification Toolkit, Contoso performed an analysis of their data and determined the following levels.

Level 1: Low business value	Level 2: Medium business value	Level 3: High business value
Data is encrypted and available only to authenticated users Provided for all data stored on premises and in cloud-based storage and workloads, such as Office 365. Data is encrypted while it resides in the service and in transit between the service and client devices. Examples of Level 1 data are normal business communications (email) and files for administrative, sales, and support workers.	Level 1 plus strong authentication and data loss protection Strong authentication includes multi-factor authentication with SMS validation. Data loss prevention ensures that sensitive or critical information does not travel outside the on-premises network. Examples of Level 2 data are financial and legal information and research and development data for new products.	Level 2 plus the highest levels of encryption, authentication, and auditing The highest levels of encryption for data at rest and in the cloud, compliant with regional regulations, combined with multi-factor authentication with smart cards and granular auditing and alerting. Examples of Level 3 data are customer and partner personally identifiable information and product engineering specifications and proprietary manufacturing techniques.

Data classification toolkit

Mapping Microsoft cloud offerings and features to Contoso's data levels

	SaaS	Azure PaaS	Azure IaaS
Level 1: Low business value	• HTTPS for all connections • Encryption at rest	• Support only HTTPS connections • Encrypt files stored in Azure	• Require HTTPS or IPsec for server access • Azure disk encryption
Level 2: Medium business value	• Azure AD multi-factor authentication (MFA) with SMS	• Use Azure Key Vault for encryption keys • Azure AD MFA with SMS	• MFA with SMS
Level 3: High business value	• Azure Rights Management System (RMS) • Azure AD MFA with smart cards • Intune conditional access	• Azure RMS • Azure AD MFA with smart cards	• MFA with smart cards

Continued on next page

Contoso's information policies

	Access	Data retention	Information protection
Level 1: Low business value	• Allow access to all	6 months	Use encryption
Level 2: Medium business value	• Allow access to Contoso employees, subcontractors, and partners • Use MFA, TLS, and MAM	2 years	Use hash values for data integrity
Level 3: High business value	• Allow access to executives and leads in engineering and manufacturing • RMS with managed network devices only	7 years	Use digital signatures for non-repudiation

Contoso's path to cloud security readiness

1. **Optimize administrator accounts for the cloud**

   Contoso did an extensive review of the existing Windows Server AD administrator accounts and set up a series of cloud administrator accounts and groups.

2. **Perform data classification analysis into three levels**

   Contoso performed a careful review and determined the three levels, which was used to determine the Microsoft cloud offering features to protect Contoso's most valuable data.

3. **Determine access, retention, and information protection policies for data levels**

   Based on the data levels, Contoso determined detailed requirements, which will be used to qualify future IT workloads being moved to the cloud.

Cloud security resources

Microsoft Cloud Security for Enterprise Architects
http://aka.ms/cloudarchsecurity

Information Protection for Office 365
http://aka.ms/o365infoprotect

Security in a Cloud-Enabled World Microsoft Virtual Academy Course
http://aka.ms/securecustomermva

Microsoft