Global Knowledge®

Expert Reference Series of White Papers

Office 365: An Introductory Guide

Office 365: An Introductory Guide

Boris Gigovic, CISSP, SSCP, MCSE, MCT, CCNA

Introduction

The cloud represents one of the most interesting topics of today's computing. The concept of practicing a centralized approach for information management that makes the cloud is not that new, and has been around since the beginning of systems interconnectivity. However, there are fundamental differences—present-day systems are being accessed by a much larger scope of clients, and the tools to manage the infrastructures are very different. Scalability, security, and mobility are required factors that have become the basics of technology meeting business requirements.

When it comes to the private cloud, it can certainly solve some problems we are facing, mainly scalability and flexibility in assigning physical resources appropriately. With virtualization being commonly present in most major infrastructures, it is becoming easier to deploy infrastructures and manage them under the same umbrella system. However, such implementations still require IT staff to deal with HA and security, as well as take care of overall health of the implementation. One example of a private cloud solution is the Microsoft System Center suite of products, which offers Virtual Machine Manager (VMM), an App Controller (cloud management tools); System Center Operations Manager (SCOM) for monitoring; Orchestrator for automation; Service Manager for IT management; and Data Protection Manager (DPM), a backup and recovery tool. These tools make a complete framework on which a private cloud can be built.

With a public cloud, managed by a third-party, many issues are solved, with the back-end administration being outsourced. Office 365 can provide benefits in scalability, security, high availability, and information access through a robust back-end platform, and is considered a reliable public cloud solution. Although the back-end is managed by Microsoft with its Azure platform, Office 365 allows a greater level of control of your resources suited to your particular needs.

Whether your organization chooses to deploy a private or public cloud infrastructure, it is certain that systems administration will change, which will require efforts by both IT staff and clients alike to adapt to this new kind of environment.

In this white paper, we will explore how one kind of public cloud system, Office 365, works. We will discover what steps your organization should choose to implement an infrastructure that is completely driven by Office 365, as well as in a scenario when some of your services need to remain within the premises of the organization, while the rest can be hosted outside the organization.

The Office 365 Products Suite

Office 365 is a set of products that works similarly to other already well-known Microsoft technology. It is delivered as a Software as a Service (SaaS) cloud solution, and uses the following products at its core:

- Exchange Server
- SharePoint Server
- Lync Server

The online version of these popular tools is made available through an Office 365 subscription, which also includes access to another popular Office application, the Office 365 ProPlus suite.

Optionally, it is possible to use the online version of the following products as well, which are available by acquiring the appropriate subscription plan:

- Yammer (successor to SharePoint, primary enterprise social utility)
- Project (enterprise project, portfolio management)
- Visio (online diagrams maker)
- Dynamics CRM (customer management)

Licensing

In a standard on-premises scenario, it is often required to follow relatively complex licensing. There is a multi-layered approach to take into consideration: from the base server to the application and the Client Access License (CAL).

The licensing model in Office 365 has been simplified to the point that there is no need to invest in any of these layers, except for the fee of the Office 365 subscription itself. One license is assigned to one user, and can be granted or revoked at any time.

Office 365 features are unlocked based on the licensing plan that is chosen. Each plan is specifically designed to cater to an organization's needs (e.g., access to Office applications, compliance, enterprise management) and limitations (e.g., the number of users supported for the plan. It is even possible to assign parts or functionalities provided by the licensing plan.

One particularly interesting option is the ability to run the full Office 365 ProPlus suite on up to five computers simultaneously. This comes with all plans except for Business Essentials and E1.

The Fast-Track Approach

Companies are conducting different phases to implement a technology, and following a specific pattern in key milestones of implementation of a product. Following the conventional method of work can take a long time before it is possible to operate the new software. And you run the risk of acquiring a specific set of licensing options that you cannot immediately use. Office 365 changes this approach by introducing ways for companies to get access sooner, get the technology running quickly, and use different tools to gradually adopt enhancements and transitioning methods.

The idea is to use a three-step approach to effectively take advantage of the acquired technology:

1. Pilot: This is the setup of the Office 365 trial platform and migration of few users over the new platform. This step focuses on being able to analyze the effectiveness of the new system by transitioning a set of users and understanding if Office 365 meets the technical and business requirements. If it does, you can convert the trial into the fully licensed product.
2. Deploy: The deploy phase aims to convert on-premises services onto cloud. This is the actual migration step for general clients. In reality, the biggest part of the work is migrating mailboxes over Office 365. A well-defined strategy is needed, and depending on the coexistence method to be used, several steps in the configuration of the messaging will have to be completed (e.g., DNS changes). Tools such as Connected Accounts help make the transition more transparent to end users.
3. Enhance: This step allows the configuration of optional components with the objective to take advantage of single sign-on (SSO) or directory synchronization options. This simplifies administration user accounts and optimizes resource access.

Initial Configuration

Setting up an Office 365 does not take much time: the licensing model is chosen, a tenant account is created, and the rest takes only a few minutes to be built. Technically, it does not involve much from your end as a systems engineer because of the very few dependencies on the actual on-premises installation.

While the environment is being created, there are still a few tasks to perform before the first users can get migrated:

1. Create accounts: This task involves populating the Office 365 environment by adding several accounts, which can be accomplished through four methods:
   - Manual creation through Office 365 Administration Center
   - CSV bulk import
   - PowerShell bulk creation
   - DirSync (AD/Office 365 synchronization)

2. Allocate licenses: Although you can import users without actually assigning a license to them, in most cases, a license is required.
3. Configure security groups: Security groups are used within some Office 365 services, such as SharePoint, for granting or denying access to resources. Creating these groups in advance is beneficial in order to allow easier access upon assignment. A group created in the root of the Office 365 installation is not the same kind of group that is used by Exchange. Exchange groups are separate distribution, mail-enabled, and dynamic, and will also need to be created and populated.
4. Define administrator roles: Users created or imported in the Office 365 do not have any administrative functions within the system. Because delegation is a feature you are likely going to implement, it is possible to assign some permissions to be used within the platform:
   - Global administrators: These users have full control over the Office 365 platform, and can alter security and permissions of other accounts.
   - Billing administrators: These delegated users deal with licensing, subscriptions, and purchases.
   - Password administrators: These users can manage service requests and reset passwords for standard accounts, but without privileges to change other administrators.
   - Service administrator: This user role can manage service requests (Exchange, SharePoint, etc.) and monitor the health of the online service.
   - User management administrator: A delegated user can manage groups, service requests, and user accounts (except higher delegated users), as well as monitor the infrastructure.

5. Configure password policies: Password expiration and/or complexity policies must be set. Providing the option for a forced password change upon a user's first login is also important.
6. Enable optional settings such as Right Management Services (RMS): RMS is used to protect internal information and prevent it from being disclosed to external recipients (in Exchange, SharePoint, and Office products). Enabling RMS at the global level initially is beneficial, if supported by the acquired subscription plan.

DNS and UPN Suffixes

The DNS system is a critical part in configuring Office 365. You will likely need to alter DNS records of the zone for email, SharePoint, or Lync services.

When you register in Office 365, Microsoft assigns the .onmicrosoft.com to the external domain name you specify; for example, yourcompany@onmicrosoft.com. The onmicrosoft.com domain will remain a temporary domain until you change the DNS records of your native domain to point to Microsoft's servers for different online services.

In fact, you will need to add your own domains in Office by proving you are the owner of these (done through a TXT record verification). Thus, you will need access to the administration panel wherever it is registered.

One confusing aspect is the domain name vs. client login name. By default, any user created will take the default companyonmicrosoft.com suffix for logging in. However, over time this will change. As you add your native domain to Office 365, you will also need to change the login suffix to reflect the native domain.

Changing the suffix without an announcement to your users will make their login fail, as their identity will change, and they will no longer be able to use the companyonmicrosoft.com suffix. Thus, some planning is required here.

Another important consideration to keep in mind is Office 365's external UPN suffix must be the same as the primary internal UPN suffix. The popular .local or .private internal domains are not supported on Office 365, thus Directory Synchronization will fail.

The result of your login name can be: firstname.lastname@company.com (company.com being added as an owned domain will appear in the list of domains used for login suffixes).

Once you've proved you own the domain and configured user logins, you will need to alter DNS for different services as explained in the following section.

Exchange

Client Access

DNS servers will also reflect a certain change for email access, especially if the name of the internal domain is the same as the external name, which is represented as a split-brain DNS scenario. Basically, your internal canonical name (CNAME) records will always point to the alternate name of the services on Office 365:

Original ExchangeCNAME record	Target CNAME record
Autodiscover.company.com	Autodiscover.outlook.com

In case of a hybrid configuration and an Exchange system remains on-premises, the A/CNAME record pointing to the client access server/array will remain the same.

Notice there is no dedicated Outlook Web Access (OWA) fully qualified domain name (FQDN). Once a mailbox has been configured, users can access email from the portal.office.com webpage (generic Office 365 landing page) or directly through mail.office365.com.

Also, A records for CAS are not used.

Email Routing

For external email routing, mail exchange (MX) records have to be changed to reflect Microsoft's servers:

Original Exchange MX record	Target Exchange MX record
***SMTP*.company.com**	Company-com.mail.protection.outlook.com

Internal routing and between on-premises and cloud (if used) does not conflict with these records, since MX records are not used for internal mail flow.

In a hybrid configuration, some scenarios might require inbound email to continue pointing to your on-premises servers. In such cases, no actions are required—email belonging to Office 365 users will be routed from your on-premises mail-flow servers to the cloud system.

Sender Policy Framework (SPF) records need to be changed to reflect the IP address of the MX record in case MX records are changed initially:

Original SPF record	Target SPF record
"v=spf1 +a +mx +ip4:(On-premises Exchange MX IP)?all"	"v=spf1 +a +mx +ip4:(Exchange online MX FQDN)?all"

Federation Services

Federation services records are used to connect the on-premises deployment to Office 365 in case of a hybrid deployment, as well as to help clients locate Exchange servers online. These records will need to point to the Office 365 system.

Lync

If the objective is to use Lync Online, records need to be altered to point to the Office 365 system.
First, a federation between two SIP domains can be created:

Service	Target
_sipfederationtls	Sipfed.online.lync.com

Lync Online also uses Service (SRV) records to manage the client infrastructure:

Service	Target
_sip	sipdir.online.lync.com

Lync clients use CNAME records to locate their online service:

Alias	Target
Sip	sipdir.online.lync.com

It is the same for mobile devices, but with a different FQDN:

Alias	Target
Lyncdiscover	webdir.online.lync.com

SharePoint

If applicable to be migrated, SharePoint requires a CNAME that provides an FQDN for a website hosted on that platform. It does not require any other type of record. In case of split-DNS, you are required to change the IP address of the FQDN internally, to be pointed to the Office 365 infrastructure.

Migration and Coexistence

Exchange

The core of the migration on Office 365 very often refers to Exchange, being probably the most important service you want to transfer or set up to work hybrid.

There are many possibilities, as some organizations decide to remove Exchange from the on-premises world completely, while in other cases that is not be possible due to compliance, regulations, or standards that specifically mention emails or archives that have to be stored/transported on-premises.

Cut-Over / Staged Migration

When the objective is to decommission the internal Exchange servers, a cut-over or staged migration is effective. Cut-over is done without coexistence, while a staged approach can be used as a mini-coexistence, without many features that are reflective of a true coexistence scenario.

Cut-over is suitable for direct transitioning, but only for a limited number of users (maximum two thousand). But, it is the simplest approach, as the migration of the mailboxes can be performed during a weekend, for example.

Due to the limited number of users that can be migrated, organizations often opt for the relatively simple staged approach. Mailboxes are moved in the same way as cut-over.

For both of these scenarios, an Office 365 account that has access to a mailbox using the Outlook Anywhere (RPC over HTTPS) will connect and retrieve the content of the mailbox and its settings, and transfer it over to a new Office 365 account.

There are a few prerequisites that have to be met:

- Mailbox access needs to be configured appropriately (OA has to be enabled).
- Security: The user account from Office 365 must have some permissions over the mailbox.
- Certificates from a third-party CA must be installed on the on-premises CAS server.
- UM must be disabled on affected mailboxes.
- Domains on which the mailbox is configured to work must be found and already verified in your Office 365 administration center.

Cross-premises / hybrid coexistence

A coexistence scenario is established when you plan to have both infrastructures running for a longer period of time. Certain regulations at the company level dictate that email (or parts of it) needs to stay local, for example. In this case, you can still take advantage of Office 365 Exchange system to offload some work, and create a trusted relationship between the components. All your servers become part of the same organisation, and you are able to route emails, share calendars, contacts, etc. between the two systems. It is also the step to take before migrating more than two thousand users.

In sum, much more integration is done between the two systems when this implementation is running. A unified management access; cross-platform mailbox transfer; OWA redirection; comprehensive delivery reports, including the two systems; and many other advantages exist when configuring an Exchange hybrid scenario.

This method also allows you to control mail flow. (If using Exchange Online, you can set Exchange Online to analyze and look for spam, and you can configure either the on-premises or cloud setup for outbound email.) It all depends on the policies that are set up at the organization level.

For email access such as OWA or Outlook, clients are redirected or proxied to whichever setup has its own mailbox. This scenario is conceptually similar to a configuration with two on-premises physical sites, where mail flow and client access is very much transparent, but can be customized to a certain extent.

Other Scenarios

There are less popular scenarios you can take advantage of to migrate your mailboxes to the cloud. If you are not using an Exchange solution internally, you can connect to that solution using the POP3 or IMAP protocol from Office 365, and proceed with extracting the content, more precisely the mailbox or messages only.

By using the PST Capture tool, you can also inject content of PST files into the Office 365 system if other methods fail or become non-applicable.

SharePoint Migration

SharePoint features the very similar interface seen on-premises in the cloud. It integrates the known types of libraries, websites, lists, and other content, such as the OneDrive. Thus, you can decide to use the online version of the platform, and remove your on-premises installation completely.

In this case, moving content to SharePoint in the cloud can be performed in the following three ways:

1. **Manual Copy**
   While this is likely the least practical scenario, it is very possible and achievable. However, some content, such as metadata, can be lost. A similar and still manual way is to use the Save As template feature, and include the content of the entire site in the template itself. Then, on the remote SharePoint system, you would need to import the template, which is the entire website from the on-premises installation in this case.

2. **Transition**
   Users, who have access to both portals, are slowly transitioning to the new system, as fewer changes happen at the on-premises installation. Over time, the on-premises setup will likely no longer be used. This is a problematic approach because it does not technically transfer the data over, but rather uses a redirection approach.

3. **Third-party Tools**
   There are third-party solutions created to perform this work. However, the rate of success in moving over large amounts of data is limited. While technically feasible, this too is a problematic approach since many organizations do not necessarily want to transition everything. In many cases, they want to be selective, but the environment has been built and maintained in such a way that it does not reflect scalability anymore. Thus, a clean-up or maintenance of some sites and data would be necessary prior to using third-party solutions.

Lync Migration

Many organizations aim to preserve Lync on-premises, while adding the Office 365 to offload some of its functionality to cloud. A much greater level of control of that VoIP system is achieved when the on-premises part is not removed, if already existent.

There are two main ways to set up an on-premises Lync environment to work with Office 365:

1. **Federated SIP**
   This approach uses a basic method of establishing a trust between two different SIP domains, and then enabling resources sharing. It is a similar approach to federating with a partner, when being exclusively on-premises. It's a relatively simple process and the overhead is low, but some features will be limited due to the fact that Lync services are in separate SIP domains. No DNS changes are required when federating (provided all was initially set up properly on the on-premises side, such as SRV records).

2. **Coexistence (SIP Sharing)**
   This newer method adds an Office 365 Lync service to the same organization. In this scenario, some users are hosted in the cloud while others are on-premises. Users can split some functionalities, provided they have this scenario, which requires the DirSync, as well as AD FS add-ons. When using SIP sharing, DNS and routing changes might be necessary to reflect how voice connectivity will occur for inbound and outbound calls.

DirSync and Active Directory® Federation Services (AD FS)

AD FS is basically a single sign-on mechanism. It allows an on-premises client to authenticate to an Office 365 system without re-authenticating on that remote system.

A trust is built between a locally established AD FS Proxy and Microsoft's AD FS servers. Internally, users install the AD FS server itself, with few other prerequisites.

Once the trust is created, a specific token from the on-premises domain is sent to the Microsoft servers. At that point, the token validity and trust is verified, and the client presents claims that act as additional information about the account itself and where it came from.

AD FS requires careful planning, since the DirSync feature is needed to make it complete.

Installing AD FS features is done separately on dedicated servers. As this is a secure system by design, it also requires the configuration of a PKI and issuance of several types of certificates.

DirSync is designed to synchronize changes between the on-premises and Office 365. To import user accounts into Office 365, install the Directory Synchronization Tool to one of the servers being members of a domain, and then create a task to upload some of the AD objects directly to the cloud.

It is possible to take advantage of password replication as well, which eliminates issues with different logins (AD FS also partially resolves this). If you have a password replication configured with DirSync, you are fully able to authenticate back and forth between on-premises and Office 365 with simply one authentication prompt.

Conclusion

Office 365 has a vast array of features to explore. We've covered the basics of these features, as well as looked at some possibilities for integrating solutions within your own organization. A rich administration interface, streamlined security, and versatile migration options make this one of the most interesting products when it comes to an SaaS public cloud solution.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Managing Office 365 Identities and Services (M20346)

Core Solutions of Microsoft Exchange Server 2013 (M20341)

Core Solutions of Microsoft Lync Server 2013 (M20336)

Core Solutions of Microsoft SharePoint Server 2013 (M20331)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Boris Gigovic is a technical consultant and the CEO of Eccentrix, a training center and solutions provider that offers skills advancement solutions and consulting services in the main areas of information technology. As an active instructor for Global Knowledge, he specializes in networking courses as well as security.

As a technical resource, Boris helps organizations maximize their investment into technology products, as well as find the best way to leverage key functionalities of these solutions. His areas of expertise are numerous, and include planning and designing computer networks, major infrastructure upgrade projects, administration, and maintenance and support of these networks.

Being a Microsoft Certified Trainer, Boris delivers courses on various technologies, including Windows operating systems, messaging tools, and communication and collaboration platforms. He dedicates some of his time to security consulting (mostly security assessments), as well as VMware and Citrix software consulting.