Microsoft 365

A reference book for administrators

Michael Lappenbusch
IT-SPECIALIST APPLICATION DEVELOPMENT

Table of contents

1.Introduction to Microsoft 365

What is Microsoft 365?

Microsoft 365 is a cloud-based suite of productivity applications from Microsoft that includes online versions of Microsoft Office applications such as Word, Excel, PowerPoint, and OneNote, as well as additional tools such as Exchange Online, Teams, and SharePoint. It allows users to access the applications from any device with internet connection and also offers features like online collaboration and cloud storage.

One of the most important features of Microsoft 365 is the ability to collaborate on documents in real time. Users can edit documents together without having to access the same physical file. This allows teams to work together effectively no matter where they are located.

Microsoft 365 also offers a range of security features, such as the ability to protect sensitive documents with a PIN and the ability to delete documents after a specified time. There are also features for managing user access rights and monitoring activities.

Microsoft 365 is available in different subscription plans that can vary depending on the needs of the company or the individual. Plans range from single user subscriptions to enterprise plans suitable for large businesses with multiple users.

In summary, Microsoft 365 is a cloud-based productivity platform that includes online versions of Microsoft Office applications as well as additional tools such as Exchange Online, Teams, and SharePoint. It allows users to edit and collaborate on documents from any device and also offers extensive security and management features. It is available in various subscription plans that cater to the needs of individuals to large corporations.

Microsoft 365 architecture

The Microsoft 365 architecture is divided into several layers that relate to the various components and services that work together to enable Microsoft 365.

The first tier is the client tier, which is the Microsoft 365 user interface. This layer includes the various applications such as Word, Excel, PowerPoint and OneNote available on various devices such as PCs, Macs, tablets and smartphones. The client layer allows users to access and edit their documents and data.

The second tier is the service tier, which provides the various Microsoft 365 services and features, such as Exchange Online, Teams, and SharePoint. These services allow users to send and receive email, collaborate as a team, and share documents and content.

The third layer is the platform layer, which provides the technical infrastructure and resources that support Microsoft 365 services and applications. This includes servers, storage and networks as well as the operating systems and databases used.

The fourth layer is the management layer, which enables the administration of Microsoft 365. This layer includes functions such as managing user accounts, monitoring activities, and configuring security settings.

The fifth tier is the data tier, which manages Microsoft 365 data storage and backup. This layer includes the various storage media such as local hard drives, cloud storage and backup systems.

All layers work together to provide a secure, reliable, and scalable platform for productivity and collaboration. Microsoft operates and maintains the Microsoft 365 environment and provides the necessary resources and services to ensure that the applications and services are always available and up to date.

In summary, Microsoft 365 architecture consists of multiple layers that relate to the various components and services that work together to enable Microsoft 365. These layers are the client layer, which represents the user interface of Microsoft 365, the service layer, which provides the various services and functions of Microsoft 365, the platform layer, which provides the technical infrastructure and resources that support the services and applications of Microsoft 365, the management tier, which enables administration of Microsoft 365, and the data tier, which manages Microsoft 365 data storage and backup. All layers work together to provide a secure, reliable, and scalable platform for productivity and collaboration.

Supported Platforms

Microsoft 365 supports a variety of platforms to make the applications and services accessible on a wide range of devices and operating systems.

In the area of desktop operating systems, Microsoft 365 supports Windows and MacOS. Office applications such as Word, Excel and PowerPoint are available as desktop applications for both platforms. There is also a web version of Office available through a browser on any operating system.

In the area of mobile devices, Microsoft 365 supports iOS and Android. There are dedicated Office apps for these platforms that allow users to access and edit their documents and data on the go.

In the area of web browsers, Microsoft 365 supports the most common browsers such as Chrome, Firefox, Safari and Edge. This allows users to access Microsoft 365 from any device as long as it has a supported browser.

In terms of managing and configuring Microsoft 365, it also supports a variety of tools and platforms. These include the Microsoft 365 admin center, PowerShell, and the Microsoft Graph API. These tools and platforms allow admins to manage and configure Microsoft 365 and customize it to their organization's needs.

In summary, Microsoft 365 is very flexible and supports a variety of platforms, such as Windows, MacOS, iOS, Android, and most popular web browsers, as well as a variety of tools and platforms for management and configuration, making it a suitable choice for companies and organizations of all sizes.

2.Planning and preparation

Hardware and software requirements

Microsoft 365 has certain hardware and software requirements that must be met in order to fully utilize the applications and services.

In terms of hardware requirements, Microsoft 365 requires a computer or mobile device with an internet connection. To use Office's desktop applications, such as Word, Excel, and PowerPoint, it is recommended that the computer has at least 1 GB of RAM and 3 GB of free disk space. To use the Office mobile apps, it is recommended that the mobile device has at least 1GB of RAM.

In terms of software requirements, Microsoft 365 supports the latest versions of Windows and MacOS. To use the Office applications on Windows computers, it is recommended that the operating system is Windows 10 or later. To use the Office applications on MacOS computers, it is recommended that the operating system is MacOS 11.0 or later.

To use the Office mobile apps on iOS devices, it is recommended that the operating system is iOS 14.0 or higher. To use the Office mobile apps on Android devices, it is recommended that the operating system is Android 6.0 or later.

When using the web version of Office, it is recommended that the browser used is a current version of Chrome, Firefox, Safari or Edge.

In terms of managing and configuring Microsoft 365, it is recommended that the tools and platforms used, such as the Microsoft 365 admin center, PowerShell, and the Microsoft Graph API, are the latest versions.

It is important to note that these requirements are the minimum requirements. For the best performance and experience with Microsoft 365, it is recommended that the hardware and software are up to date.

Planning of user and service accounts

Planning the user and service accounts is an important step in implementing Microsoft 365. Creating the right accounts for the right users and services is necessary to ensure all users have the necessary access rights and resources to do their jobs to carry out successfully.

First, user accounts should be created. These accounts should be created for each user who will be using Microsoft 365. It is important to ensure that each user has a unique account and that accounts are securely and uniquely identified. Some companies use email addresses as sign-in credentials, while other companies use their own usernames.

After the user accounts have been created, service accounts should be created. These accounts are used to gain access to specific services and resources within Microsoft 365, such as Exchange Online, SharePoint Online, OneDrive for Business, and Teams. Service accounts should be created for each service to be used and it is important to ensure that the accounts are secure and uniquely identified.

It is also important to carefully plan the access rights for the user and service accounts. This includes setting permissions for specific services and resources, as well as setting roles and permissions for managing Microsoft 365.

Another important consideration when planning user and service accounts is security. It is important to ensure that all accounts are protected with strong passwords and that accounts are regularly reviewed to ensure they are not being misused.

It's also important to consider authentication and access requirements. This includes using two-factor authentication, using single sign-on, and using remote access solutions.

Planning user and service accounts requires careful thought and preparation to ensure all users have the necessary access rights and resources to do their jobs successfully.

Microsoft 365 organization theme

Microsoft 365 organization design refers to the structure and organization of Microsoft 365 within a company or organization. It includes the planning and configuration of services, resources and access rights to ensure that users' requirements and needs are met.

An important consideration in the design of the Microsoft 365 organization is the structure of the services and resources. This includes setting permissions for specific services and resources, as well as setting roles and permissions for managing Microsoft 365.

Another important element in the design of the Microsoft 365 organization is the structure of users and groups. This includes creating user and group accounts, assigning permissions and roles, and creating security groups to control access to specific services and resources. This enables only authorized persons to access certain data and functions.

Another important element in the design of the Microsoft 365 organization is planning for network connectivity and security. This includes planning firewall rules, VPN connections, and other network security settings to ensure data in Microsoft 365 is safe and secure.

Another important element in the design of the Microsoft 365 organization is planning backup and recovery strategies. This includes creating backup copies of Microsoft 365 data and running tests to ensure disaster recovery is successful.

Another important element in the design of the Microsoft 365 organization is planning for identity and access management. This includes using single sign-on, using two-factor authentication, and using remote access solutions to ensure only authorized individuals have access to Microsoft 365.

Overall, the design of the Microsoft 365 organization requires careful thought and planning to ensure that user requirements and needs are met and that data in Microsoft 365 is safe and secure.

3.Installation and Configuration

Installing Microsoft 365

Installing Microsoft 365 refers to the process of setting up and configuring Microsoft 365 on a computer or mobile platform. There are different ways to install Microsoft 365, depending on whether it's a stand-alone installation or a bulk installation.

One way to install Microsoft 365 is to use the Microsoft 365 installer. This installer is downloadable and allows you to install Microsoft 365 on a computer or mobile platform.

Another way to install Microsoft 365 is by using the Office Deployment Tool. This tool makes it possible to install and configure Microsoft 365 in bulk. It makes it possible to automatically adapt and distribute Microsoft 365 to the needs of an organization.

Another way to install Microsoft 365 is to use Microsoft Intune. This makes it possible to install and manage Microsoft 365 on mobile devices.

An important aspect of installing Microsoft 365 is the configuration of the services and resources. This includes setting permissions for specific services and resources, as well as setting roles and permissions for managing Microsoft 365.

Another important aspect of installing Microsoft 365 is configuring network connections and security. This includes setting up firewall rules, VPN connections, and other network security settings to ensure data in Microsoft 365 is safe and secure.

Another important aspect of installing Microsoft 365 is configuring identity and access management. This includes using single sign-on, using two-factor authentication, and using remote access solutions to ensure only authorized individuals have access to Microsoft 365.

It's also important to perform regular maintenance after installing Microsoft 365 to ensure applications and services are kept up-to-date and secure. This may include performing updates, monitoring for security vulnerabilities, and conducting tests.

Overall, installing Microsoft 365 requires careful planning and configuration to ensure that users' needs and requirements are met and that data in Microsoft 365 is safe and secure. It is also important to perform regular maintenance to ensure applications and services are always up-to-date and secure.

Configure network components

Configuring network components is an important aspect of setting up Microsoft 365 because it ensures data is safe and secure and that users have access to the services and resources they need.

An important aspect when configuring network components is setting up firewall rules. This makes it possible to control access to Microsoft 365 and ensure that only authorized people have access to the services and resources. It's important to create firewall rules for the various Microsoft 365 services and resources, such as Exchange Online, SharePoint Online, and Teams.

Another important aspect when configuring network components is setting up VPN connections. This makes it possible to securely access Microsoft 365 from external locations. It's important to use the right VPN protocols and configurations to ensure data is transmitted securely.

Another important aspect when configuring network components is the configuration of DNS entries. This makes it possible to resolve Microsoft 365 services and ensure users are accessing the correct services and resources. It's important to create the correct DNS records for the various Microsoft 365 services and resources, such as Exchange Online, SharePoint Online, and Teams.

Another important aspect of configuring network components is monitoring and managing network connectivity and security. This includes monitoring firewall rules, VPN connections, and other network security settings to ensure data in Microsoft 365 is safe and secure and that users have access to the services and resources they need.

Overall, configuring network components requires careful planning and configuration to ensure that user requirements and needs are met and that data in Microsoft 365 is safe and secure. It is also important to regularly monitor and manage network connections and security to ensure applications and services are always up to date and secure. It is also a good idea to create network documentation to record and maintain the configurations that are used.

It is important that the IT department or an experienced network administrator performs the configuration of the network components to ensure that the security and performance of the network is not compromised.

It's also important to read Microsoft documentation and use Microsoft Technical Support to ensure the Microsoft 365 installation is properly configured.

Create Microsoft 365 organizations and locations

Creating Microsoft 365 organizations and locations is an important process when setting up Microsoft 365. It enables Microsoft 365 data and resources to be organized and managed to meet security and compliance requirements.

A Microsoft 365 organization is a group of users, resources, and services that are brought together to provide unified management and security. An organization can have multiple locations divided into different geographic regions or business units.

To create a Microsoft 365 organization, you must first purchase a Microsoft 365 subscription. Once you have a subscription, you can use the Microsoft 365 admin center to create a new organization. You will be prompted for information such as organization name, number of users, and preferred language.

After the Microsoft 365 organization is created, you can add locations. A site is a geographic region or business unit that groups users and resources together. To add a location, you must use the Microsoft 365 admin center and provide information such as the location name and associated users.

It is important to carefully plan and configure the organization and locations to ensure that user requirements and needs are met and that data and resources are properly organized and managed. It is also important to regularly monitor and manage the organization and locations to ensure they are always up to date and secure. It is recommended that organization and site documentation be established to record and maintain the configurations that are used.

Also, an important part of creating Microsoft 365 organizations and locations is configuring security and compliance settings. These settings can be used to protect the data and resources from unauthorized access and data loss. This includes, for example, enabling multi-factor authentication, using encryption technologies and setting up data protection policies.

It is important that the IT department or an experienced administrator handles the creation of the Microsoft 365 organizations and locations to ensure that the security and performance of the network is not compromised.

It's also important to read Microsoft documentation and use Microsoft technical support to ensure the Microsoft 365 organizations and locations are created correctly.

4. Management of User Accounts and Services

Creating and managing user accounts

Creating and managing user accounts is an important process in managing Microsoft 365. It allows users to access Microsoft 365 services and resources and manage their activities.

To create a user account in Microsoft 365, you must first ensure that you have the necessary permissions to create and manage user accounts. Once you have permissions, you can use the Microsoft 365 admin center or PowerShell to create a new user account. You will be prompted for information such as the user's name, email address, and password.

After the user account is created, you can manage it by using the Microsoft 365 admin center. Here you can perform actions such as changing the password, assigning licenses, and assigning security groups. It is also possible to manage user accounts with PowerShell, but this is intended for advanced users and requires knowledge of PowerShell.

It is important that Microsoft 365 user accounts are properly created and managed to ensure users can access the services and resources they need and to keep Microsoft 365 secure. It is also important to regularly monitor and manage user accounts to ensure they are always up to date and secure. It is good practice to create user account documentation to record and maintain the facilities that are used. It's also important to consider security policies and compliance requirements related to user accounts, such as using complex passwords, enabling multi-factor authentication, and establishing policies for data protection.

It is important that the IT department or an experienced administrator handles the creation and management of user accounts to ensure that the security and performance of Microsoft 365 is not compromised. It is also important to read Microsoft documentation and use Microsoft technical support to ensure user accounts are properly created and managed.

In summary, the steps to create and manage user accounts in Microsoft 365 are:

Verify that you have the required permissions to create and manage user accounts.

Use the Microsoft 365 admin center or PowerShell to create a new user account and provide the required information.

Use the Microsoft 365 admin center or PowerShell to manage the user account by performing actions such as changing the password, assigning licenses, and assigning security groups.

Regularly monitor and manage user accounts to ensure they are always up to date and secure.

5. Create documentation of user account setup and administration.

Consider security policies and compliance requirements related to user accounts, such as using complex passwords, enabling multi-factor authentication, and setting privacy policies.

Let the IT department or an experienced administrator handle the creation and management of user accounts.

Read Microsoft documentation and use Microsoft technical support to ensure user accounts are properly created and managed.

It is important that user account management in Microsoft 365 is carefully planned and executed to ensure users have access to the resources and services they need and to ensure Microsoft 365 security. It is also important that user accounts are regularly monitored and managed to ensure they are always up to date and secure.

Creating and managing services (e.g. Exchange Online, SharePoint Online, Teams)

Creating and managing services in Microsoft 365 is an important aspect of running a Microsoft 365 organization. Some of the major services available in Microsoft 365 are Exchange Online, SharePoint Online, and Microsoft Teams.

Exchange Online is a cloud-based email service that supports email, calendar, contacts, and tasks. It can be managed through the Microsoft 365 admin center or PowerShell cmdlets. It is important that the IT department or an experienced administrator configures and manages Exchange Online to ensure that email communications are secure and reliable.

SharePoint Online is a cloud-based service for collaboration and content sharing. It allows users to store documents, collaborate, share content and manage projects. It can be managed through the Microsoft 365 admin center or PowerShell cmdlets. It is important that the IT department or an experienced administrator configures and manages SharePoint Online to ensure content is secure and properly organized.

Microsoft Teams is a cloud-based collaboration platform that supports chat, calling, video conferencing, document sharing, and more. It can be managed through the Microsoft 365 admin center or PowerShell cmdlets. It is important that the IT department or an experienced administrator configures and manages Microsoft Teams to ensure that collaboration in the organization is smooth and secure.

Some of the key tasks involved in managing services in Microsoft 365 are:

Configure and manage the services using the Microsoft 365 admin center or PowerShell cmdlets.

Establish policies for using the Services to ensure they are used safely and effectively.

Monitor use of the Services to ensure they are being used appropriately and to identify and resolve potential issues.

Consult Microsoft documentation and use Microsoft technical support to ensure the services are properly configured and managed.

It is important that management of services in Microsoft 365 is carefully planned and executed to ensure users have access to the resources and services they need and to ensure Microsoft 365 is secure. It is also important that the Services are regularly monitored and maintained to ensure they are always up to date and secure.

Delegated Access Rights

Delegated access rights in Microsoft 365 allow administrators to give other users the ability to perform specific tasks on behalf of another user. This is particularly useful when an administrator is not available every day or when certain tasks need to be performed by other users on a regular basis.

There are different types of delegated access rights available in Microsoft 365, including:

Calendar delegation: A user can give other users the ability to view, edit, or add their calendar entries.

Email delegation: A user can give other users the ability to view, edit, or reply to their email inboxes.

Task delegation: A user can give other users the ability to see, edit or add their tasks.

Contact delegation: A user can give other users the ability to view, edit, or add to their contact list.

Delegated access rights can be set up either through the Microsoft 365 admin center or through settings in Outlook. It is important for the administrator to ensure that the correct access rights are granted to the correct users and that the users who are given delegated access rights have the knowledge and skills required to perform the tasks properly. It is also important that delegated access rights are regularly reviewed and adjusted to ensure they always reflect current needs.

It's also important to note that delegated access rights can compromise Microsoft 365 security if not managed properly. Therefore, it is important for the administrator to ensure that all delegated access rights are secure and that the users who are granted them understand how to use them securely.

Services Access Policies

In Microsoft 365, there are several ways to create and manage service access policies. Some of the main methods are:

Using Azure Active Directory (Azure AD): Azure AD is Microsoft 365's identity and access management system. Azure AD allows administrators to create and manage access policies that control how users sign in to Microsoft 365 services.

Using Exchange Online Management: Exchange Online is the Microsoft 365 email and calendar service. Exchange Online Management allows administrators to create and manage access policies that control the use of email and calendaring features.

Using SharePoint Online Administration: SharePoint Online is the collaboration and document management service of Microsoft 365. With SharePoint Online Administration, administrators can create and manage access policies that control the use of SharePoint sites and documents.

Use of Microsoft Teams Admin: Microsoft Teams is Microsoft 365's chat and teamwork service. Microsoft Teams Admin allows admins to create and manage access policies that govern how Teams is used and what it can do.

Using Cloud App Security: Cloud App Security is a cloud-based security tool that enables administrators to create and manage comprehensive access policies for Microsoft 365 services.

Access policies can vary depending on the needs and requirements of the organization. For example, a policy can specify that only authorized users can access certain documents or folders in SharePoint Online, or that certain users are not allowed to receive email attachments from certain senders. It is important that access policies are regularly reviewed to ensure they are always up to date and that they adapt to the changing needs of the organization.

Another important concept when creating access policies for Microsoft 365 services is the use of role-based access control (RBAC). RBAC allows administrators to assign users specific roles that give them specific access rights to Microsoft 365 services. This allows administrators to easily manage and change users' access rights without having to manually adjust each individual access policy.

Overall, it is important that access policies for Microsoft 365 services are carefully planned and implemented to ensure that the services can be used securely and productively, while maintaining organizational security and compliance.

5. Management of message flows and security

Configure transport rules

Transport rules are rules used in Exchange Online (the Microsoft 365 email and calendar service) to filter and process incoming and outgoing email. Transport rules allow administrators to take specific actions when certain conditions are met, such as deleting emails that contain specific tags or sending emails to a specific group of recipients.

To configure transport rules in Exchange Online, administrators must first use Exchange Online PowerShell to connect to the Exchange Online service. Once connected, administrators can use commands to create, edit, and delete transport rules.

A transport rule consists of a condition and one or more actions. The condition describes the e-mail properties to which the rule should be applied, such as the presence of certain keywords in the subject or in the body of the e-mail. The actions describe the actions to be taken when the condition is met, such as deleting or moving emails to a specific folder.

There are many different types of transport rules that can be used in Exchange Online, such as rules to block email from specific senders or domains, rules to protect against spam and phishing emails, and rules to send automatic replies to specific recipients.

It is important that the transport rules are carefully planned and tested before being deployed in a production environment, as an incorrectly configured rule can lead to undesirable results. It is also important to regularly review the transport rules and adapt them to the changing needs of the company.

Overall, transport rules in Exchange Online enable administrators to more effectively control and protect email communication in the company by filtering unwanted emails and automatically forwarding important emails to the right recipients.

Configure anti-spam and anti-malware protection

Anti-spam and anti-malware protection are key Microsoft 365 features that help protect the business from unwanted email and malicious software.

Anti-spam protection in Microsoft 365 uses multiple technologies to detect and block unwanted email. This includes:

Using IP reputations: Microsoft 365 checks email sender IP addresses and blocks email from IP addresses known to be spam senders.

Use of keywords and patterns: Microsoft 365 searches the content of emails for keywords and patterns that indicate spam, such as "Viagra" or "winning notification".

Using Bayesian filters: Microsoft 365 uses artificial intelligence to classify emails as spam or ham (legitimate email traffic) based on their content.

Anti-malware protection in Microsoft 365 uses multiple technologies to detect and block malicious software, including:

Using signatures: Microsoft 365 uses a constantly updated database of signatures from known types of malware to detect malicious files.

Use of heuristics: Microsoft 365 uses heuristic technologies to detect and block suspicious files based on their behavior.

Use of cloud-based analysis tools: Microsoft 365 uses cloud-based tools that help detect malware in email attachments and SharePoint files.

Configure mail flow controls

Mail flow controls are an important part of email security in Microsoft 365, helping to control and regulate the flow of mail in an organization.

Some of the key mail flow controls that can be configured in Microsoft 365 are:

Transport rules allow admins to block or redirect specific emails based on criteria like sender, recipient, subject line and more.

Recipient policies allow administrators to block specific email recipients from receiving email from specific senders.

Sender policies allow administrators to block specific email senders from sending email to specific recipients.

Journaling rules allow admins to send a copy of all emails sent or received in the organization to a specific email address.

Retention Policies allows admins to set how long messages should be retained in specific mailboxes and when they should be automatically deleted.

It's important to note that the exact method for configuring mail flow controls in Microsoft 365 can vary by service and organization. It's a good idea to read Microsoft's documentation and ensure controls are properly configured to ensure security and control of mail flow in the organization.

Configure security policies

Security policies are an important part of security in Microsoft 365 and help minimize the risk of data loss, data leakage, and security breaches.

Some of the key security policies that can be configured in Microsoft 365 are:

Access control allows admins to block specific users or groups from accessing specific services or data in Microsoft 365.

Authentication allows admins to ensure only authorized users can access Microsoft 365 services by enforcing the use of multi-factor authentication.

Encryption enables admins to ensure data is transmitted and stored securely in Microsoft 365 by enforcing the use of encryption for email and files.

Malware protection enables admins to mitigate the risk of malware attacks on Microsoft 365 services by using malware detection and blocking tools.

Data Loss Prevention (DLP) enables administrators to minimize the risk of data loss by creating rules to monitor and block the transmission of sensitive data.

It's important to note that the exact method for configuring security policies in Microsoft 365 can vary by service and organization. It's a good idea to read Microsoft's documentation and ensure security policies are properly configured to minimize the risk of security breaches in the organization.

Configure authentication methods

Authentication is an important part of security in Microsoft 365 and enables administrators to ensure that only authorized users can access Microsoft 365 services.

There are several methods to configure authentication in Microsoft 365, including:

Password policies allow administrators to set rules for how passwords are used, such as minimum length, required character types, and password rotation frequency.

Multi-factor authentication (MFA) allows administrators to augment user authentication by using multiple factors, such as passwords and smartphone push notifications.

Authenticator apps allow users to verify their identity using an app on their smartphone or tablet.

Smart card authentication allows users to confirm their identity using a smart card.

Federated Identity allows administrators to delegate user authentication to an external identity management system.

It's important to note that the exact method of configuring authentication in Microsoft 365 can vary by service and organization. It's a good idea to read Microsoft's documentation and ensure authentication is properly configured to minimize the risk of security breaches in the organization.

6. Management of data storage

Manage storage plans

Managing storage plans in Microsoft 365 is an important aspect of running an organization. The right storage plans can ensure users have enough storage space for their documents and data without spiraling out of control over storage costs.

In Microsoft 365, there are several ways to manage storage plans:

Microsoft 365 plans: Microsoft 365 plans offer a fixed amount of storage for each user, which varies by plan. Microsoft 365 plans include Microsoft 365 Business Essentials, Microsoft 365 Business Premium, and Microsoft 365 Enterprise E3.

SharePoint storage plans: SharePoint storage plans enable administrators to manage storage space for SharePoint Online sites.

Exchange Online storage plans: Exchange Online storage plans allow administrators to manage storage space for Exchange Online mailboxes.

It's important to note that storage plans for Microsoft 365, SharePoint, and Exchange Online are different and must be managed separately. It's a good idea to read Microsoft's documentation and ensure storage plans are properly configured to ensure users have enough storage space and that storage costs stay within budget.

There are also ways for admins to monitor and analyze users' storage usage and allocations in Microsoft 365, for example by using PowerShell cmdlets or the Microsoft 365 admin portal.

Managing Databases

Managing databases in Microsoft 365 is an important aspect of an organization's operations because it enables data to be stored and accessed effectively and securely.

In Microsoft 365 there are several ways to manage databases:

Microsoft SQL Server: Microsoft 365 offers the ability to host and manage Microsoft SQL Server databases in the cloud, known as Azure SQL Databases. This allows developers to create, modify, and manage databases without having to worry about the infrastructure.

SharePoint Databases: SharePoint Online provides the ability to create and manage databases known as lists. This allows users to store and retrieve data in a simple and intuitive manner.

Exchange Online Databases: Exchange Online uses databases to store messages, calendars, and contacts. These databases are created and maintained automatically when an Exchange Online mailbox is created.

It's important to note that how databases are managed in Microsoft 365 depends on the type of database and service used. It is advisable to read Microsoft's documentation and ensure that the databases are properly configured to ensure that data can be stored and retrieved safely and that the performance of the databases is adequate.

There are also ways for admins to monitor and analyze database usage and performance in Microsoft 365, for example by using PowerShell cmdlets or the Microsoft 365 admin portal.

Manage backups and restores

Managing backups and restores in Microsoft 365 is an important aspect of an organization's operations because it enables data to be recovered in the event of data loss or corruption.

Microsoft 365 offers several ways to manage backups and restores:

Exchange Online: Exchange Online offers the ability to backup and restore mailboxes by moving messages to an archive or restoring them from the recycle bin. There is also the option to export and restore entire mailboxes.

SharePoint Online: SharePoint Online provides the ability to back up and restore site collections and document libraries by restoring content that has been deleted from the Recycle Bin or by exporting and restoring entire site collections.

Microsoft Teams: Microsoft Teams provides the ability to backup and restore teams and channels by restoring content that has been deleted from the recycle bin or by exporting and restoring entire teams.

It's important to note that how backups and restores are managed in Microsoft 365 depends on the service used and the type of data.

It is also important to run regular tests of the recovery features to ensure that the data can be correctly recovered should it be needed.

Microsoft 365 also offers the ability to set up automated backups that are created on a regular basis to ensure current data is always backed up. There is also the option to use external backup solutions that integrate with Microsoft 365 to provide an additional layer of protection.

When managing backups and restores in Microsoft 365, it's also important to consider the organization's data protection and compliance requirements and to ensure that data is backed up and restored in accordance with those requirements.

In summary, managing backups and restores in Microsoft 365 is an important aspect of running an organization to ensure data can be recovered in the event of loss or damage. It is important to read Microsoft's documentation and ensure backups and restores are properly configured, conduct regular testing, and consider the organization's data protection and compliance needs.

7.Monitoring and Troubleshooting

Configure monitoring options

When configuring monitoring options in Microsoft 365, there are several ways to monitor and analyze the operation and usage of the services. Some of these monitoring options include:

Microsoft 365 logging: This makes it possible to log activities in Microsoft 365, such as email messages, calendar entries, file changes, and more, and use this data for analysis and monitoring.

Microsoft 365 reports: There are a variety of reports available in Microsoft 365, such as mail flow reports, user activity reports, and more, that provide insight into service usage and help identify potential issues.

Microsoft 365 security and compliance reports: These reports provide insights into security and compliance activities in Microsoft 365, such as possible threats, unusual activities, and more.

Microsoft 365 Auditing and Alerting Policies: These policies make it possible to monitor specific activities or events and receive alerts when they are triggered.

Microsoft 365 Management API: This API makes it possible to programmatically monitor and analyze Microsoft 365 activities by providing the ability to retrieve and process data from Microsoft 365.

It is important to choose the right monitoring options to meet the organization's specific requirements and needs. It's also important to regularly review and adjust monitoring options to ensure they always reflect current needs. It's also important to ensure that the monitoring options are configured correctly to ensure they deliver the expected results.

Another important aspect of managing Microsoft 365 monitoring options is documentation. It is important to document the configuration and results of monitoring options to ensure they can be traced in the event of a problem or query.

It is also important to educate staff to understand and use the monitoring options correctly. This includes training employees on how to interpret the reports they receive and identify potential problems or threats.

Overall, configuring and managing monitoring options in Microsoft 365 is an important part of keeping the services running securely and efficiently, and it's important to choose the right monitoring options and regularly review and adjust them to ensure they always meet current needs.

Manage logs and reports

Managing logs and reports in Microsoft 365 is an important aspect of the secure and efficient operation of the Services. Logs and reports provide important information about the use and performance of the Services, as well as possible problems or threats.

An important step in managing logs and reports is selecting the right logs and reports. Microsoft 365 offers a variety of logs and reports that can be used for various purposes. It is important to select the logs and reports that are best suited to the organization's specific needs.

Another important step in managing logs and reports is the configuration of the logs and reports. It is important to configure the logs and reports to provide the expected results. This includes configuring the reports to ensure they contain the information you want.

Another important step in managing logs and reports is monitoring and analyzing the logs and reports. It is important to regularly review and adjust logs and reports to ensure they always reflect current needs. It is also important to analyze the logs and reports to identify and fix possible problems or threats.

Another important step in managing logs and reports is documentation. It is important to document the configuration and the results of the logs and reports to ensure the information is easily accessible for future reference. Documentation can be in the form of notes, technical documents or wiki pages.

It is also important to review the logs and reports for compliance requirements. Depending on the industry and business area, certain logs and reports may need to be retained for a specific period of time.

Finally, it is important to ensure the security of the logs and reports. It is important to ensure that only authorized persons have access to the logs and reports and that the logs and reports are protected against unauthorized access.

Overall, the management of logs and reports in Microsoft 365 is an important aspect of the safe and efficient operation of the services. By selecting, configuring, monitoring, analyzing and documenting the logs and reports, organizations can ensure they are getting the results they expect and can identify and resolve problems or threats early.

Troubleshoot problems

Troubleshooting Microsoft 365 issues is an important aspect of running a Microsoft 365 organization. There are many potential issues that can arise in a Microsoft 365 environment, from simple configuration errors to complex technical issues.

One of the most important steps in troubleshooting Microsoft 365 issues is identifying the problem. This can be done by monitoring logs and reports, collecting information from users, or running tests. Once the problem has been identified, it is important to determine the impact of the problem and whether it requires emergency treatment.

Once the problem has been identified and impact determined, troubleshooting can begin. This can be done by applying workarounds, updating software, or making configuration changes. It's also important to document the problem and record the steps that were taken to resolve the problem.

An important aspect of troubleshooting issues in Microsoft 365 is also preventing issues. This can be done by performing maintenance, applying security updates, and running tests. It's also important to have processes and procedures in place to identify and fix problems before they affect users.

Overall, troubleshooting issues in Microsoft 365 is an important aspect of running a Microsoft 365 organization. By identifying, resolving, and preventing problems, organizations can ensure their Microsoft 365 services remain stable and available.

8.Upgrades and Migrations

Upgrade to newer versions of Microsoft 365

Upgrading to a newer version of Microsoft 365 is a process that can vary depending on the scope and type of upgrade. Here are some steps to consider when upgrading to a newer version of Microsoft 365:

Planning: Before beginning the upgrade, you should create a comprehensive plan that includes the nature of the upgrade, the users affected, the business impact, and the steps to prepare for, perform, and track the upgrade.

Preparation: Before you start the upgrade, you should make sure that all required updates and patches are installed on all computers and devices that use Microsoft 365. It is also important to create all the backups and data you need to be able to restore the data in case of a problem.

Implementation: The actual upgrade process can vary depending on the scope and type of upgrade. It can be a simple upgrade of a single application or service, or it can be a major upgrade of the entire Microsoft 365 tenant. During the upgrade process, you should ensure that all users are aware of the progress of the upgrade and that there is no business impact.

Follow-up: After the upgrade, you should conduct a comprehensive review to ensure that all features are working properly and that there is no impact to users or business operations. It is also important to do all the necessary customizations and configurations to ensure that the new version works smoothly and meets all the needs of the business.

Migrate from older versions of Microsoft 365

Migrating from older versions of Microsoft 365 to the latest version requires careful planning and execution to minimize business disruption. The first step in the migration process is to assess the current environment and identify the specific version of Microsoft 365 that is currently in use. This information is necessary to determine the compatibility of the current environment with the new version and to identify possible issues that may arise during the migration process.

Once the current environment has been assessed, a migration plan can be created that includes the steps and timeline for the migration. This plan should include the users, services, data, and applications that will be affected by the migration.

During the migration itself, it is important to keep users informed of the progress and any impact on their work. It is also important to provide test environments to ensure that the new version works properly and meets all of the company's requirements before implementing it in the production environment.

After the migration is complete, data and services should be validated for integrity and users trained to ensure they are able to use the new version of Microsoft 365 successfully. It is also important to regularly monitor and maintain the environment to ensure the new version is running smoothly and meeting all the needs of the business.

Migrating from other cloud services to Microsoft 365

Migrating from other cloud services to Microsoft 365 can be a complex process that requires careful planning and execution. There are different methods for migration depending on the service and data to be migrated.

One method is to use tools like Microsoft FastTrack or Azure Migration, which are specifically designed for migrating data and services to Microsoft 365. These tools automate many steps of the process and can significantly reduce migration times.

Another method is to use third-party tools tailored to the specific needs of the data and services being migrated. For example, these tools can support the migration of email data from another email service or the transfer of documents from another cloud storage service.

It's also important to carefully plan the target Microsoft 365 subscription to ensure it has sufficient resources and capacity to support the migrated data and services.

A key step in the migration is also preparing users by educating them about the upcoming move and educating them on how to work with the new Microsoft 365 services and capabilities.

A comprehensive testing strategy should also be implemented throughout the process to ensure that all data and services are properly migrated and that there is no post-migration impact to users or business operations.

Full documentation of the process and results should also be created to facilitate traceability and to ensure that all steps can be repeated in future migrations.

9.Advanced Configurations

Configure Microsoft 365 federated sharing

Microsoft 365-federated sharing enables organizations to share their content and resources with external users without requiring them to have their own account in the organization. To configure Microsoft 365 federated sharing, there are a few steps to follow:

Setup of an Active Directory Federation Services (AD FS) or other SAML-based authentication provider: This is required to manage authentication of external users.

Configure domains and identity providers: The domains to be used in Microsoft 365 federated sharing and the identity providers to be used must be configured.

Configure SharePoint Online Sharing: In SharePoint Online, the settings for sharing content with external users must be configured.

Configure Exchange Online Sharing: In Exchange Online, the settings for sharing calendars and contacts with external users must be configured.

Configure OneDrive sharing: In OneDrive, the settings for sharing files with external users must be configured.

Testing the configuration: It's important to test the Microsoft 365 federated sharing configuration to ensure it's working correctly and that external users can access the resources they want.

It's important to note that configuring Microsoft 365 federated sharing requires some technical knowledge and it's recommended that you hire an experienced IT professional to implement it.

Configure Microsoft 365 hybrid scenarios

Microsoft 365 hybrid scenarios enable companies to connect their existing on-premises environments to the Microsoft 365 cloud environment. This makes it possible to combine the advantages of using the cloud with the existing investments in on-premises systems.

To configure a Microsoft 365 hybrid scenario, certain steps must be performed:

Preparation: Verify that the necessary hardware and software requirements are met. Make sure Active Directory is ready and has the necessary synchronization and authentication roles.

Microsoft 365 Hybrid Wizard: This tool helps you configure the hybrid connection between on-premises and Microsoft 365. You can use it to create the connection between your on-premises

environment and Microsoft 365, the necessary services to enable and configure and set up synchronization of user and group accounts.

Exchange Hybrid: It is necessary to have Exchange 2010 SP3 or higher in the on-premises environment to take advantage of the hybrid functionality of Exchange. This configuration makes it possible to merge and manage mailboxes from the cloud and on-premises.

SharePoint Hybrid: To enable SharePoint hybrid scenarios, you must have SharePoint Server 2013 or higher in the on-premises environment and perform the necessary hybrid configurations. This makes it possible to merge and manage SharePoint content from the cloud and on-premises.

A Microsoft 365 hybrid scenario allows companies to connect their existing on-premises environments to Microsoft 365 cloud services. With a hybrid configuration, organizations can take advantage of Microsoft 365 while maintaining their existing IT investments.

To configure a Microsoft 365 hybrid scenario, organizations must first set up a hybrid connection server. This server connects the on-premises environment to the Microsoft 365 cloud services and enables synchronization of user accounts and mailboxes.

It is important that the on-premises environment meets the minimum Microsoft 365 requirements to ensure a successful configuration. This includes, among other things, a current version of Microsoft Exchange, Active Directory and .NET Framework.

Once set up, organizations need to activate and configure the Microsoft 365 services they want to use. This includes Exchange Online and SharePoint Online, companies can also set up rules for data flow control and security as well as for authentication.

It is also important that the IT department regularly monitors the synchronization of user accounts and mailboxes and makes adjustments as necessary. Ongoing monitoring and maintenance of the hybrid configuration is required to ensure Microsoft 365 service users are able to work smoothly.

Configure Microsoft 365 archive mailboxes

Microsoft 365 archive mailboxes are a feature that allows you to swap out old emails, calendar entries, and contacts to save storage space in your primary mailbox. These archive mailboxes can be configured through the Microsoft 365 admin center or PowerShell.

First, create a new archive mailbox rule in the Microsoft 365 admin center. To do this, go to Mailboxes > Mailbox Policies in the management console and create a new policy.

Configure the rule by specifying when emails should be automatically moved to the archive (e.g. after 30 days).

Now assign an archive mailbox policy to users. You can do this either for individual users or for groups of users.

To access the archive mailbox, users must open their primary mailbox in Outlook and then switch to the archive mailbox.

Optionally, you can also configure retention management settings to automatically delete old emails from the archive.

It is important to note that the archive mailboxes may incur additional costs and that there may be some restrictions on access to the archive mailboxes and their content. It is therefore advisable to carefully examine the requirements and costs before configuring archive mailboxes.

Configure Microsoft 365 compliance options

Microsoft 365 offers various compliance options to help companies comply with legal regulations and corporate policies. This includes:

Content Search: This feature allows admins to search for specific content in emails, OneDrive files, and SharePoint documents. It enables the identification of content that violates company policies and the monitoring of potential compliance risks.

Retention Policies: Retention Policies allow admins to set how long specific types of content should be retained before being automatically deleted. This enables companies to comply with legal retention periods.

Litigation Hold: This feature allows admins to "freeze" specific email inboxes or OneDrive files to ensure they are not deleted or modified while a legal case is pending.

Data Loss Prevention (DLP): With DLP, administrators can create rules to ensure certain types of sensitive information, such as credit card or social security numbers, are not inadvertently shared.

Azure Information Protection: This solution allows administrators to automatically classify and protect documents and emails to ensure they can only be read by authorized people.

It is important to note that configuring these compliance options requires administrators to carefully examine their organization's legal requirements and corporate policies and set the appropriate settings and rules.

imprint

This book was published under the
Creative Commons Attribution-NonCommercial-NoDerivatives (CC BY-NC-ND) license released.

This license allows others to use and share the book for free as long as they credit the author and source of the book and do not use it for commercial purposes.

Author: **Michael Lappenbusch**

E-mail: admin@perplex.click

Homepage: https://www.perplex.click

Release year: 2023