

Multi-Tenancy and Hosting Guidance

Exchange Server 2013

February 2013

Contents

[Terms and Definitions Used in This Document 3](#_Toc348515707)

[Executive Summary 4](#_Toc348515708)

[Solving the Challenges Associated With Multi-Tenancy 5](#_Toc348515709)

[Provisioning and creation of objects 7](#_Toc348515710)

[Establishing Security Boundaries 13](#_Toc348515711)

[System Wide Settings and Policies 16](#_Toc348515712)

[Transport 23](#_Toc348515713)

[Features and functionality 28](#_Toc348515714)

[Design and Architecture considerations 31](#_Toc348515715)

[Scalability 35](#_Toc348515716)

[Migration From Other Exchange Hosting Solutions 41](#_Toc348515717)

[Exchange 2010 /Hosting to Exchange 2013 41](#_Toc348515718)

[HMC to Exchange Server 2013 41](#_Toc348515719)

[Multi-Tenant Scale Guidance 41](#_Toc348515720)

[Appendix 42](#_Toc348515721)

[Legal Notice 43](#_Toc348515722)

## Terms and Definitions Used in This Document

|  |  |
| --- | --- |
| Term | Definition |
| Exchange 2013 | A standard Exchange Server 2013 installation. |
| Exchange 2010 | Exchange Server 2010 with Service Pack 2 installed without use of the /Hosting switch, providing a single tenant installation. This is the default installation mode for Exchange Server 2010. |
| Exchange 2010 /Hosting Mode | Exchange Server 2010 SP1 or later installed using the /Hosting switch, which provides built-in multi-tenant features and tenant isolation |
| Tenant | A tenant is a customer of the service. A tenant could be made up of one user, or a group of users. All users within that one tenant typically have full visibility of each other. Users within one tenant cannot see users from other tenants despite being on the same system. |
| Service Plan | A service plan allows you to enable or disable certain features when deploying tenant organizations. They simplify tenant administration by automatically setting up feature configuration and automatic feature provisioning of mailboxes. |
| HMC | The Solution for Hosted Messaging and Collaboration (HMC) which incorporates Microsoft Exchange Server, Microsoft Windows SharePoint Services and Microsoft Office Communications Server (in HMC 4.5). HMC also includes a provisioning system used to simplify and automate the tenant creation and management processes. |
| RBAC | Role Based Access Control (RBAC) is the permissions model introduced in Microsoft Exchange Server 2010 and later versions. |
| Resellers | Resellers have administrative control over tenants created below them in the system hierarchy. Essentially the hoster delegates some level of control to the reseller who manages a subset of the hosters’ tenants. |
| PowerShell/Exchange Management Shell | The Exchange Management Shell, built on Windows PowerShell technology, provides a powerful command-line interface for Microsoft Exchange Server 2010 and 2013 that enables automation of administrative tasks. |

## Executive Summary

A multi-tenant Exchange deployment is defined in this document as one where the system has been configured to host multiple and discrete organizations or business units (the tenants) that ordinarily do not share e-mail, data, users, global address lists, or any of the other commonly used objects in Exchange.

There are many challenges to overcome when you try to use Exchange 2010 or 2013 to host tenants. Exchange server has always been designed to enable all users in the Exchange organization to collaborate easily, and creating boundaries between tenants means going against some of the core principles used in the design and development of the product.

With this caveat in mind, it is still possible to create a configuration that appears to be multi-tenant; however, doing this in a supportable manner can be difficult.

This document does not provide step-by-step instructions about how to achieve multi-tenancy with Exchange 2013, but provides information on the challenges and problems that need to be solved, and offers advice and direction to ensure the Exchange environment you build can be supported by Microsoft.

This document also refers to Exchange 2010 in places in order to highlight similarities, differences, because the guidance either has some relevant version dependency, or because it relates to both Exchange 2010 and Exchange 2013. This document provides guidance for Exchange 2010 when co-existing with Exchange 2013 and in that scenario, this guidance detailed in this document supersedes that published for Exchange 2010.

Many of the features built in to Exchange 2013 will continue to function as they were designed regardless of any changes an administrator makes to configure it for multi-tenancy. A feature may work in the way it was designed, but unfortunately it might not be in a way the administrator intended. This document highlights many of those cases, explains reasons for why it might happen, and recommends if the feature should be configured in a certain way or perhaps not used at all. If you decide to accept and use the feature regardless of the recommendation, you will not be able to obtain support from Microsoft for the lack of functionality or any leakage of data between tenants that may result.

In order for your multi-tenant Exchange solution to be considered fully supported, you must follow all the guidance stated in this document and in any existing published Microsoft documentation. If you chose to deviate from the guidance provided in this document or the standard documentation you will be unable to obtain support from Microsoft for part, or all of your solution.

This guidance does change over time and so we recommend you ensure you are reading the latest version of the guidance at all times.

## Solving the Challenges Associated With Multi-Tenancy

The challenges that need to be overcome when building a multi-tenant solution using Exchange Server 2013 fall into several key areas:

* **Provisioning and Creation of Objects**   Once the system is deployed and customers begin to use the service, probably the most overlooked yet fundamentally important aspect begins – the operation of the platform, and that begins with provisioning and creation of objects. Making sure that objects are created in the right way, in the right place, and with the right settings is imperative to successfully operating a hosted Exchange environment. Building tools and scripts to enable operators to produce repeatable and auditable results is fundamental, but ensuring those tools are built on supported technologies is just as important if you want to run a fully supported configuration.
* **Establishing Security Boundaries**   This covers many different features, but in the simplest terms it is about ensuring that a user from one tenant on the system cannot see users or data from another tenant on the system. This is referred to in this guidance as establishing security boundaries and covers many different features and functions of Exchange, as well as ensuring that the platform is designed from the ground up with tenant security in mind. For example, it begins with the initial layout of the Organizational Unit hierarchy in Active Directory, ensuring that delegation of administration can be achieved but ensuring that permission is not given to Organizational Units outside of the scope of an admin. Further up in the application stack, establishing security boundaries means ensuring the results of a query that a client application makes to the system return only results from the same tenant. And further still, establishing security boundaries means considering how to prevent data being exposed between two tenants who communicate, when both their mailboxes are hosted on the same underlying system.
* **System-wide settings and policies**   Exchange has many features available to end users and administrators alike, and these can be set and controlled in many different ways. Some of these settings are configured on a per-user basis, some can be controlled at the database level, some are policies that can be applied to a collection of objects, and some are set globally for the entire Exchange Organization. These system wide settings and policies affect things such as the actions a user can perform with the Outlook Web App (OWA) client, what cross-organization options are available, as well as settings and policies consumed by mobile devices used to access mailboxes.   
    
  Some of these settings can be set once and affect every user on the system; some can be overridden by more granular or scoped settings on a policy or per-user basis. This document lists many of these settings and provides guidance on the configuration you should use, and also highlights which can be overridden on a more granular level.
* **Transport**   Another system wide consideration is transport. Some transport settings are stored at the organizational level, some at the individual level, but in addition to these settings, there are some challenges associated with the standard way Exchange resolves addresses to recipients when people exchange e-mail in a multi-tenancy configuration. This presents problems for hosters when two tenants sharing the same platform start communicating as Exchange treats them as though they were both part of the same tenant, and tries to provide the same rich experience it was designed to provide.
* **Features and functionality**Most of the issues discussed up to now relate to the overall system configuration, ensuring system wide settings are appropriate for users, or using more granular settings if appropriate. From the user’s perspective most of these changes are invisible and happen behind the scenes. They care most about features and functionality, what they can and cannot do with their client and mailbox. Exchange is a feature rich system, users can perform many tasks and actions, and most that have previously used the more recent versions of Exchange are familiar with features such as MailTips and setting an Out-Of-Office (OOF) message.   
    
  Some of these features present problems when trying to configure Exchange to host multiple tenants. These features assume all users on the platform are peers and internal to each other and so the feature that allows a user to set an internal OOF and an external OOF and ask Exchange to deliver the correct message when required, relies on Exchange and the user having the same concept of internal and external.   
    
  The Exchange Control Panel, new since Exchange 2010, provides a user with ways to set and change their configuration, but it can also be used to allow additional tasks such as distribution group management and discovery and search to be used. Some of these features can’t be made to work in the same way as they do in a single tenant configuration when Exchange is configured for multi-tenancy.
* **Design and Architecture considerations**This refers to configuring the generic service names used for things like OWA access, URLs provided to Outlook clients, the service endpoint used for AutoDiscover requests, and the hostname used by Outlook Anywhere. These values can be seen by all clients and should be generic in nature, preferably non-branded to avoid future problems.   
    
  Consideration also needs to be given to other applications which will exist in the same forest, another forest, whether trusted or not, or any location where services are obtained or provided. For instance, if you want to host Exchange, SharePoint and Lync, you need to understand their inter-dependencies and any constraints one application places on the other. If you fail to fully map out all dependencies prior to deployment you will possibly have to retrace your steps, causing disruption to your service and processes.
* **Scalability**Another key attribute in designing the platform is planning for scalability of the solution you deploy. Scalability is not simply about the maximum size the system can attain, it’s about understanding various limits and constraints related to Exchange and then predicting how they work together to limit the size the system can grow to or the maximum load the system can operate under. Related aspects are capacity planning and sizing – planning for target tenant numbers, and predicting growth of the system towards the scale limits and determining how the system will continue to adapt in a way that avoids hitting those limits.

Within each of these areas there are various challenges to overcome and solve. The following sections detail these issues and provide guidance where appropriate. Some of these issues exist in some way in multiple sections, and some of the solutions you may choose to develop may span categories, the taxonomy is being used only to generally group the items in a logical fashion.

**NOTE:** While every effort has been made to make this list as comprehensive as possible, it still may not include everything you need to consider when designing and building the solution. We welcome your feedback and comments and will incorporate them into future versions if required. If you have feedback, please send it to [ExHostingFeedback@microsoft.com](mailto:ExHostingFeedback@microsoft.com).

### Provisioning and creation of objects

One of the first challenges to solve is ensuring that the creation of tenant related objects is consistent, supported and achieves consistent results. Mistakes in this area might result in clients that are unable to connect, users exposed to data from other tenants, and difficulty in troubleshooting. Fortunately it is relatively simple to ensure object creation is simple and consistent if fundamental principles and good practices are observed.

|  |  |
| --- | --- |
| Problem or Issue Description | Ensuring a reliable and repeatable provisioning process is followed. |
| Recommended Approach | Thoroughly tested automation and processes are the keys to building a supported and successful solution.  Provisioning solutions that Mail-enable (or mailbox-enable) objects must leverage the Exchange Management Shell, Console or Administration Center. Standard interfaces such as the Active Directory Module for Windows PowerShell, WMI, and VBScript are supported for object creation in Active Directory.  There are no other recommendations other than ensuring you follow a standard methodology in your tool and process development, using known and supported interfaces and methods. |
| Unsupported Solutions | Any attempts to manipulate, change or otherwise override the configuration options that are normally available using the built-in cmdlets available in the Exchange Management Shell or the Exchange Administration Center will be unsupported. For example, directly manipulating objects in Active Directory using any method when the same result can be achieved by using an Exchange recipient cmdlet will be unsupported. |
| Additional Comments | Though Exchange Server 2013 and Windows provide both a user interface and cmdlet based tools for creation and management of objects, it is recommend that your solution develops a set of scripts and processes that are used to create, remove and manage tenant objects. For example, when a new tenant is added to the system, you could create a script that creates an organizational unit in Active Directory using PowerShell for Active Directory, and include steps to create a security group for restricting access to tenant objects, then use the Exchange Management Shell to create an address list, a global address list (GAL), and an offline address book (OAB). Using scripts that call known and supported commands ensures the process is repeatable, auditable and supportable.  Once the process is in place it is also important to ensure that no other methods of object creation are used unless the operator is certain they will not cause adverse side effects. For example, if a new mailbox is created and the address book policy (ABP) assignment is accidentally forgotten, that mailbox will have access to the Default GAL, potentially exposing all users on the platform.  One way to solve this could be to build a solution using RBAC or build a custom management tool, but it is unlikely that technology is going to prevent accidents like this from ever happening as the administrators still need high level access to the system. It is imperative that adequate thought be given to training administrators and ensuring defined procedures are consistently followed.  If you choose to use a product such as Microsoft’s Forefront Identity Manager 2010 R2 product as part of your provisioning solution you may want to review the material available at <http://technet.microsoft.com/en-us/magazine/ff472471.aspx> which offers some advice on using the tool to properly provision Exchange recipient objects.  It’s also important to consider all provisioning operations as transactional, so that proper error handling and rollback is built in to the process. Exchange generally handles this within its cmdlets, but any provisioning workflow you build will result in the execution of multiple cmdlets. For example, if your workflow for creating a new tenant involves creating several objects such as accepted domains, an Organizational Unit, and security groups you need to consider what will happen if one of those steps fails. If your logic simply removes all failed objects it may allow you to re-run the script but you may hit issues with Active Directory replication and be unable to re-create them. Alternatively, if your provisioning engine is able to rollback individual steps within a process, you may find it makes provisioning easier to restart. |

|  |  |
| --- | --- |
| Problem or Issue Description | Management of objects to ensure supportable results. |
| Recommended Approach | The only supported way to manage objects that will be used on the platform is by using the built in tools and management interfaces provided by Exchange or Windows.  For example, creation or management of mail-related objects can only use the built-in Exchange PowerShell cmdlets such as New-Mailbox and New-MailContact.  All Exchange PowerShell sessions must be initiated via a Remote PowerShell (RPS) connection to an Exchange 2013 (or above) server unless managing the Exchange Server 2010 Edge Transport server role, which uses only Local PowerShell sessions.  Due to the way Remote PowerShell and Role Based Access Control work together you may need to configure OU permissions to allow manipulation of AD objects to take place.  For creation of objects such as Organizational Units, you can use the Active Directory Module for Windows PowerShell or any language or script that uses ADSI or LDAP.  It is strongly recommended that you run all cmdlets or tools in verbose mode or allow it to be easily enabled to aid in troubleshooting efforts.  In order to create a consistent, high-bandwidth connection to Remote PowerShell you should consider some combination of Runspace (i.e. – session) Pooling and ensure you build in good exception handling.  If you pool runspaces you can have multiple connections to one-or-multiple servers which will allow the most concurrent operations. Be aware though that multiple domain controllers might be being used when pooling runspaces and so your script should be able to deal effectively with any resulting timing issues.  Depending on the volume of provisioning activity on the system, it may be worthwhile to isolate the servers which are responsible for the PowerShell operations associated with provisioning activity from the servers which are responsible for handling Exchange workload transactions. For smaller implementations, this will likely not be necessary. Pre-production validation can help to determine the performance impact of peak provisioning load on the overall system.  It is also extremely important to build in general exception handling that can detect if the session has failed or is not responding and handle it gracefully (retry, recycle, etc.).  Building in the ability to temporarily disable provisioning activity in case the system is temporarily overloaded (i.e. prioritizing the user experience for existing customers rather than the speed of onboarding new customers) would also be considered a best practice for a hosted multi-tenant solution. |
| Unsupported Solutions | Any solution that attempts to bypass the standard object creation or management process will be unsupported. This includes code that attempts to create objects directly in Active Directory and then set parameters on them to make them appear to Exchange as though they were created in a supported way.  If the origin of any objects you create cannot be traced back to supported tools they will not be supported. |
| Additional Comments | It may seem tempting to use direct calls into Active Directory to directly manipulate Exchange objects, rather than re-develop existing code to use the cmdlets built in to the product. This shortcut approach may appear to work, but as code changes are made to Exchange, the gap between what worked when the solution was built and what happens now can get wider, until the approach used simply fails to work or produces unexpected results.  Microsoft makes changes to the inner workings of Exchange regularly, and not all of those changes are documented (particularly if it is in an area where we expect people *only* to use the tools we provide to execute a task). Clearly it becomes very possible over time that changes can be made that can impact code written to essentially emulate the result of running a cmdlet.  Overview of Exchange Management Shell - <http://technet.microsoft.com/en-us/library/bb123778(v=exchg.150)> |

|  |  |
| --- | --- |
| Problem or Issue Description | Implementing a service plan to enable or disable features for tenants or mailboxes. |
| Recommended Approach | A service plan is primarily a tool for selling a level of service or functionality to a tenant, backed by a series of configuration tasks and settings which call standard cmdlets and interfaces. These changes should be scripted or automated to ensure reliability and repeatability.  A value that represents the applied service plan could optionally be stored on the active directory object, ideally in one of the unused extension attributes, so that future adjustment of service plans can be performed in a simple, deterministic way. |
| Unsupported Solutions | Any attempts to manipulate, change or otherwise override the configuration options that are normally available using the built-in cmdlets available in the Exchange Management Shell or the Exchange Administration Center will be unsupported. |
| Additional Comments | A Service Plan is a collection of settings and parameters that can be applied to any set of mailboxes or tenants. It usually defines what features are enabled or disabled based on the amount of money paid for the service.  There is no built in service plan functionality into Exchange Server 2013, so you need to develop a set of configuration tasks that effectively result in a consistent experience for all users assigned to the same plan.  This might include enabling or disabling features such as Outlook access, POP and IMAP access (all of which can be simply configured using the Set-CASMailbox cmdlet), right through to determining mailbox and message size limits (easily set using Set-Mailbox).  Your service plan or plans will comprise of a large number of settings, based on many of the settings discussed elsewhere in this document. |

|  |  |
| --- | --- |
| Problem or Issue Description | Creating a self-service portal for tenant administrators. |
| Recommended Approach | The built-in Exchange Server 2013 Administration Center was not built to be multi-tenant aware when configuring Exchange to work in a multi-tenant way as described in this document.  Some features in EAC are configurable and can be enabled or disabled with the assignment or removal of RBAC roles. Some features will not respect the ABPs assigned to users, and may risk exposing data from other tenants on the system.  We recommend you disable EAC access to tenants and build your own custom control panel which calls into the underlying cmdlets and interfaces. |
| Unsupported Solutions | Attempting to modify any of the files or code that go into ECP/EAC is unsupported. |
| Additional Comments | It is recommended to completely disable access to the Exchange Administration Center by modifying the **Set-ECPVirtualDirectory –AdminEnabled** parameter on all tenant-facing Client Access servers. |

|  |  |
| --- | --- |
| Problem or Issue Description | Billing customers for usage. |
| Recommended Approach | There are no billing features built in to Exchange, but there are many data points available in the system if you choose to use them to generate usage statistics, and then determine usage and billing information.  This level of analysis places a load on the system, but if you decide this kind of service is part of your solution you should investigate the built in cmdlets such as Get-MailboxStatistics and Get-ActivesyncDeviceStatistics which provide data specific to your request, and look at things like transport logs and IIS logs, which require additional processing and analysis to be useful. |
| Unsupported Solutions |  |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Distributing mailboxes across databases. |
| Recommended Approach | When you create or move a mailbox we recommend you allow Microsoft Exchange Server 2013 to choose the target database for you by using automatic mailbox distribution unless you have good reason for locating specific mailboxes on specific databases.  Depending on the scale of the hosted deployment, it may be necessary to occasionally rebalance users across mailbox databases to provide optimal performance for the users of the system. On an extremely large scale system, random distribution may be sufficient to distribute load evenly across mailbox servers. Careful performance monitoring and capacity planning/trending are extremely important here.  A properly planned and configured multi-tenant Exchange system does not need to segregate each tenant’s mailboxes onto dedicated (per-tenant) databases to achieve multi-tenancy. It is not recommended you group tenant mailboxes in specific databases for this reason, as a problem with a single database may result in a much greater impact on those tenants.  If you need to prevent databases from being used for tenant mailboxes, you can use prevent their inclusion in the automatic distribution easily using built-in documented features. |
| Unsupported Solutions |  |
| Additional Comments | Control Automatic Mailbox Distribution Using Database Scopes - <http://technet.microsoft.com/en-us/library/ff628332.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Enabling Resellers. |
| Recommended Approach | If a hoster chooses to enable Resellers when using Exchange 2013 for multi-tenancy, they should be very aware of the risks this poses. The hoster should become very comfortable with tools such as RBAC, understand what is possible when Access Control Lists (ACLs) on address list and GAL objects are not supported, possibly create custom portals to enable configuration management, and at all times ensure their tenants data integrity. |
| Unsupported Solutions | Any ACLs or manipulation of objects not explicitly stated elsewhere in this document as being supported, are unsupported. |
| Additional Comments |  |

### Establishing Security Boundaries

Ensuring each tenant on the system can only see its own objects and not those of any other tenant is fundamental to the concept of multi-tenancy. There are many ways a client can interact with the system, using a multitude of clients or methods, and so each must be considered separately. In addition to solving the problem of ensuring an authenticated user can only access data appropriate for their own tenant, you need to ensure that any unauthenticated access does not expose recipient or tenant data.

|  |  |
| --- | --- |
| Problem or Issue Description | Providing e-mail directory access when using a supported client. This includes supported versions of Outlook, OWA, mobile devices that use the ActiveSync protocol and clients that use Exchange Web Services (EWS). |
| Recommended Approach | Address book policy objects are the only supported solution to ensure an authenticated user can access only their own tenant’s GAL, OAB and address list objects.  One or more ABP objects can be created per tenant and assigned to the users as they are provisioned.  ABPs can be used to control GAL, OAB and address list object access for clients that client accesses Exchange with an Outlook client (Windows or Mac), EWS application, a mobile device or OWA.  Having both ACLs and ABPs are only supported for the length of a migration from one to the other. |
| Unsupported Solutions | Any ACL changes on the GAL or address list objects in Active Directory will be unsupported. This includes removal of low level (Authenticated Users) read access while leaving System level ACLs in place.  It is not supported once any migration from ACLs to ABPs has completed to leave the legacy non-standard ACLs in place. |
| Additional Comments | It is important to understand that the GAL specified in the ABP is the effective scope of the user’s directory access. If you choose to create an ABP with multiple address lists, you should ensure the GAL is a superset of those address lists for predictable results. |

|  |  |
| --- | --- |
| Problem or Issue Description | Providing address list and GAL access to e-mail clients that leverage LDAP for directory access. |
| Recommended Approach | If you must provide LDAP access to clients, we recommend you create an accessible LDAP instance for each client using, for example, Active Directory LDS configured with directory synchronization to your production directory, appropriately secured for each tenant, and containing only the data that tenant needs to access.  We do not recommend you publish your Active Directory to all clients, and do not support you doing this by configuring ACLs on your Active Directory to restrict what each client can see. |
| Unsupported Solutions | Any ACL changes on the GAL or address list objects in Active Directory will be unsupported. This includes removal of low level (Authenticated Users) read access while leaving System level Access Control Entries (ACEs) in place. |
| Additional Comments | Outlook Mac 2011 can perform many directory lookup actions either by using the local OAB, or via EWS. If the LDAP server is unreachable to a Microsoft Outlook for Mac 2011 client it will use EWS.  Active Directory Lightweight Directory Services (LDS) Overview - <http://technet.microsoft.com/en-us/library/cc754361(WS.10).aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Directory harvesting attacks by using a dictionary or brute force attack to crack usernames and passwords. |
| Recommended Approach | Proactively monitor for distributed denial of service (DDOS) attacks and password brute force attacks.  Encourage (and optionally enforce) strong passwords and passphrases for all users. |
| Unsupported Solutions |  |
| Additional Comments | If account lockout policies are enabled, it becomes very simple to lockout accounts from the Internet. Often the attacker is not necessarily targeting a specific account, they are targeting any account, using a combination of usernames and passwords – the chance of succeeding is far higher when all accounts are targeted rather than one specific account. Once one account is compromised it provides an entry to the system and it may provide information about how account names are formed.  We strongly recommend you consider not using account lockout policies, and instead use strong passwords and passphrases and monitoring. |

|  |  |
| --- | --- |
| Problem or Issue Description | Securing Offline Address Book web distribution folders. |
| Recommended Approach | It is not possible to further restrict access to OAB folders beyond the default of only allowing Authenticated Users access. In Exchange 2013 access to OAB downloads are no longer performed in the context of the System and so ACL’s, as used in earlier versions of Exchange, no longer function.  It is recommended you monitor OAB access and use it to identify potential security issues. |
| Unsupported Solutions | It is unsupported to make ACL changes to the OAB container, objects, folders or sub-folders. These changes will not be respected by Exchange and may cause other issues. |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Changing default calendar permissions.  The default permission on a mailbox calendar allows Free/Busy availability to be shown to anyone on the same system who requests it. |
| Recommended Approach | It is recommended you change the default permission on a mailbox calendar to not allow the ‘Default’ user any access, but to allow other users within the same tenant to see it.  This can be accomplished either with the use of the Set-MailboxFolderPermission cmdlet, or by use of a bulk editing tool such as ExFolders. |
| Unsupported Solutions | Any method of changing permissions which does not use the built in cmdlets or the ExFolders tool. |
| Additional Comments | Mail Enabled Universal Security Groups can be added to calendar permission lists, and so your provisioning process should ensure the calendar for any users have only the appropriate permissions applied to only allow access to users from within the same tenant.  To avoid issues with converted groups and being unable to use those groups for permissions, it is recommended that you create the group as a mail enabled security group in Exchange. If you create a distribution group and then security-enable it in Windows you may be unable to use it. |

|  |  |
| --- | --- |
| Problem or Issue Description | Creating Organizational Unit hierarchies to support tenants and delegation of administration. |
| Recommended Approach | It is recommended that you design and deploy an Organizational Unit hierarchy to enable you to easily manage and segment the tenants you create on the system.  If you plan on integrating other applications with Exchange, such as Lync, we recommend you consult that product’s documentation, as they may have specific Organizational Unit hierarchy requirements.  Be careful of blocking inheritance or removing access to any built-in system accounts, these can cause unexpected results. Rather than extensively manipulate the permissions set on the Organizational Unit hierarchy, aim to use clients that do not see the Organizational Unit structure (any Exchange client using a mailbox on Exchange 2010 or later uses ABPs) or search the Active Directory directly.  If you are providing access to clients through a Remote Desktop interface, you may also need to enable Active Directory List Object Mode, for example, to prevent users from seeing all users on the system when they attempt to secure access to folders and files. |
| Unsupported Solutions | Setting the *msExchQueryBaseDN* on any user object for any reason is not supported with Exchange Server 2010 or later. |
| Additional Comments | ABPs do not rely on Organizational Unit hierarchy to control what a user can see in the directory, though other applications may.  Active Directory List Object Mode - <http://msdn.microsoft.com/en-us/library/ms675746(VS.85).aspx> |

### System Wide Settings and Policies

Many settings in Exchange are configured per Exchange Organization and the settings apply to all users hosted on that system. This has far reaching consequences if you do not consider how each of these will impact your users. Many of these settings also have more granular settings available in a policy, or that can be configured on a per-mailbox or other object level. It is recommended that the organization wide settings you configure should accommodate all tenants, and then you use more granular policies or settings to restrict individual tenants or sets of users.

For example, if the largest message you want to allow to be transmitted across the Exchange organization boundary is 50MB, set the organization wide settings to 50MB. If you then want to control which tenants can send messages that large or smaller, based on a service plan or some other mechanism, you can issue more specific policies on a per-user basis, which will override the organization wide setting. However, if you then have the need for a single tenant to send or receive a messages larger than 50MB across the organization boundary then the organization wide setting must be increased to the value the single tenant needs and then all other tenant per-user level settings previously using the organization defaults would have to modified to 50MB or else they would inherit the larger values configured for the single tenant.

This section highlights many of the settings that apply at an Organizational level, which are policy based and which have some form of override mechanism.

|  |  |
| --- | --- |
| Problem or Issue Description | Federation, Federation Delegation, Organizational Relationships and Sharing Policies are configured per-organization, not per tenant. |
| Recommended Approach | Federation, Federation Delegation, Organizational Relationships and Sharing Policies were not designed to work with Exchange configured for multi-tenancy.  Enabling Federation for your hosted Exchange 2013 solution will add significant complexity to your deployment. In most multi-tenant deployments this feature set will not work properly and risks exposing tenant data. If you do not fully understand how Federation and Federated Delegation will work as part of your solution we do not recommend enabling any of the features as you may risk exposing data between tenants.  If you decide to establish Federation with the Microsoft Federation Gateway (MFG), you should carefully plan how you configure the feature to ensure it does not expose tenant data without consent and understand that Microsoft will not accept requests to change the behavior seen when using this feature set in a multi-tenant configuration.  One Federation Trust only can be configured between your Exchange deployment and MFG. Domains can be configured on that Federation Trust to control from which domains users can use the Federation Trust relationship. DNS TXT records must be configured for each DNS zone you configure. |
| Unsupported Solutions | Any attempts to manipulate, change or otherwise override the configuration options that are normally available using the built-in cmdlets available in the Exchange Management Shell or the Exchange Administration Center will be unsupported. |
| Additional Comments | You should investigate Organization Relationships vs. Sharing Policies in order to configure your system appropriately and determine if either can be used in your specific solution.    Although Organization Relationships and Sharing Policies allow sharing of free/busy information with external users, they're intended for different scenarios. Organization Relationships are created to collaborate with external federated organizations and are limited to sharing only free/busy information. Sharing policies govern what calendar and contact information your users can share with users in external federated organizations, non-federated Exchange organizations, non-Exchange organizations, and anonymous users.  Organizational Relationships can be scoped only for inbound requests, not outbound. For example, if your solution has 10 tenants configured and one of those tenants requests you establish an Organizational Relationship with Contoso, all of your tenants now have an Organizational Relationship with Contoso. Contoso can apply a scope to choose which of their user’s free/busy information can be seen, but all of your tenants would be able see it.  Sharing Policies are person to person and therefore are less likely to leak tenant data, but they do not provide free/busy information in the same way. A user can open a calendar and look for a convenient time for a meeting, but not just see the free/busy information as they would for another user in the same tenant.  Federation - <http://technet.microsoft.com/en-us/library/dd335047.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Hybrid Relationships are set once per organization. |
| Recommended Approach | Establishing a hybrid relationship with Office 365 is not recommended if you have configured Exchange 2013 for multi-tenancy as it may expose data between tenants.  The Hybrid Configuration Wizard and the configuration used to establish a Hybrid relationship with Office 365 was not designed to work with Exchange 2013 in a multi-tenant configuration. |
| Unsupported Solutions | It is not supported to configure or attempt to configure your Exchange 2013 organization to have a hybrid relationship with multiple Office 365 tenants.  It is not supported to modify the provided directory sync solution or configure your own Directory Sync solution between Exchange 2013 and Office 365 to try and restrict the objects that are in scope of replication. |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | MailTips settings are configured once per-organization or once per Organizational Relationship. |
| Recommended Approach | In a multi-tenant configuration using Exchange 2013 we recommend you disable MailTips rather than risk exposing data between tenants.  If you disable the MailTips functionality entirely you should also disable Group Metrics generation to reduce the load on the generation server – you can do this with the Set-OrganizationConfig cmdlet. You may also notice warnings in Outlook if you completely disable MailTips.  If you choose to leave MailTips enabled to avoid the warnings, ensure your organizational level settings are appropriate for all tenants on the system, and examine the many options available for configuring MailTips for all user scenarios to ensure no unnecessary data can be exposed between tenants.  For example, you might leave MailTips globally enabled, ensure you don't set personal MailTips, and set the large audience threshold to the max of 1000 so it rarely triggers. As long as you don't have any groups with more than 1000 members, MailTips is still enabled, but not issuing any warnings. |
| Unsupported Solutions | Any attempts to manipulate, change or otherwise override the configuration options that are normally available using the built-in cmdlets available in the Exchange Management Shell or the Exchange Administration Center will be unsupported. |
| Additional Comments | MailTips - <http://technet.microsoft.com/en-us/library/jj649091.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Manipulating the *ShowInAddressBook* property of a recipient object to include or exclude it from address lists and GALs. |
| Recommended Approach | Do not use the *ShowInAddressBook* attribute to control which address lists and GALs an object appears in. Use standard filters on address list and GAL objects which will include all objects matching the filter. |
| Unsupported Solutions | Using *only* the *ShowInAddressBook* attribute to control the address lists and GALs an object appears in and not using filters on address list and GAL objects. |
| Additional Comments | In HMC configuring the *ShowInAddressBook* attribute rather than using built in filters for address list and GAL objects was standard practice to avoid the issues of provisioning with large numbers of address list and GAL objects. These issues do not exist in Exchange Server 2013. In HMC this configuration also often resulted in support issues when specific address list and recipient management cmdlets were used as these broke the configuration being used. If the filters are set correctly, provisioning will work as expected, and cmdlets will not break the configuration. |

|  |  |
| --- | --- |
| Problem or Issue Description | The hierarchical address book (HAB) root settings are stored at the organizational level, and HAB does not properly work alongside ABP. |
| Recommended Approach | It is recommended you do not provide the HAB feature to your tenants when Exchange is configured for multi-tenant hosting as you may risk exposing data between tenants. |
| Unsupported Solutions | Any attempts to manipulate or change the default way to configure HAB to attempt to allow this feature to work will be unsupported. |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Some Exchange ActiveSync settings are organization wide. |
| Recommended Approach | Ensure your organizational settings are most permissive (typically allowing all devices expect those you know to be problematic), and use more scoped device access rules for further restrictions or personal overrides.  Use Set-CASMailbox to provide allow/block control to individual mailboxes. |
| Unsupported Solutions | Any attempt to configure device access rules using any method other than the built-in cmdlets is unsupported. |
| Additional Comments | Set-CASMailbox - <http://technet.microsoft.com/en-us/library/bb125264> |

|  |  |
| --- | --- |
| Problem or Issue Description | Some EWS settings are configured at the Organization level. |
| Recommended Approach | Plan your policies such that the most permissive settings are set at the Organization level, and more restrictive policies are configured per user, using Set-CASMailbox. |
| Unsupported Solutions |  |
| Additional Comments | Set-OrganizationConfig - <http://technet.microsoft.com/en-us/library/aa997443.aspx>  Set-CASMailbox - <http://technet.microsoft.com/en-us/library/bb125264>  Set-OrganizationConfig and Set-CASMailbox include the following EWS related settings;   * *EwsAllowEntourage* * *EwsAllowList* * *EwsAllowMacOutlook* * *EwsAllowOutlook* * *EwsApplicationAccessPolicy* * *EwsBlockList* * *EwsEnabled*   Note that if *EWSEnabled* is left at the default setting *Null*, all other settings are ignored. *EWSEnabled* must be set to True for the more granular settings to take effect, or to False to disable all EWS access. |

|  |  |
| --- | --- |
| Problem or Issue Description | Outlook Web App and Exchange ActiveSync Mailbox policies can only be configured at the organizational level. |
| Recommended Approach | It is recommended you configure global settings on a per virtual directory basis. It is possible to have multiple virtual directories on one server if you need to expose multiple settings for specific tenants, but not generally recommended as it increases complexity and makes troubleshooting more complex.  It is recommended that you also configure OWA and Exchange ActiveSync Mailbox Policies and to suit either each tenant, or any service plan you create, and assign these to users during mailbox provisioning. |
| Unsupported Solutions | Any other method of changing the options available to a user in OWA or ActiveSync is unsupported. This includes editing or changing any of the files that are used for OWA or ActiveSync, or directly editing any of the attributes stored in Active Directory for each user object |
| Additional Comments | OWA settings can be configured on a per-virtual directory level using Set-OwaVirtualDirectory - <http://technet.microsoft.com/en-us/library/bb123515>  ActiveSync settings can be configured on a per-virtual directory level using Set-ActiveSyncVirtualDirectory - <http://technet.microsoft.com/en-us/library/bb123679>  Per-User settings can be set using Set-CASMailbox - <http://technet.microsoft.com/en-us/library/bb125264>  Using a policy enabled during mailbox creation is the easiest and most reliable way of changing per-user settings, as any subsequent changes apply to all users configured with the policy. |

|  |  |
| --- | --- |
| Problem or Issue Description | Voicemail journaling switch is per Exchange organization. |
| Recommended Approach | It is recommended that you enable this option if you have any tenants that require journaling and require these specific message types be captured.  There is an additional consideration however, if this setting is enabled, it will capture voicemails from all tenants. Tenants that did not request voicemail journal reports will now find this data returned in a discovery request.  We recommend you develop a solution that ensures journal reports are only enabled for those tenants that request the feature on an as-needed basis for tenants using a solution such as tenant specific transport rules. |
| Unsupported Solutions |  |
| Additional Comments | Managing Journaling - <http://technet.microsoft.com/en-us/library/aa998649(v=exchg.150).aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Retention policies and tags are configured per Exchange organization. |
| Recommended Approach | It is recommended that you configure retention policies to suit either each tenant, or each service plan you define, and assign these to users during mailbox provisioning.  It is recommended your Retention Policy Tags use generic names such as “Delete after 2 years” or “Move to Personal Archive after 1 Year” or “Deleted Items delete after 90 days” and do not include any tenant specific information in their names.  If you decide to allow users to add their own optional tags using ECP (by assigning them the *MyRetentionPolicies* Role) they will be able to see all configured tags configured on the system. |
| Unsupported Solutions | Any attempt to configure retention polices, tags, or apply mailbox settings using any method other than the built-in cmdlets and tools is unsupported. |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Configuring message classifications. |
| Recommended Approach | It is recommend that you only create generic classifications for your tenants, and allow all users to access all classifications. |
| Unsupported Solutions | It is unsupported to modify the ACLs on message classification objects in Active Directory to control which users can access those objects. |
| Additional Comments | Message Classifications - <http://technet.microsoft.com/en-us/library/bb124400.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Stamping e-mail address onto mailboxes. |
| Recommended Approach | Each time a recipient object is modified and saved, Exchange enforces the correct application of the e-mail address criteria and settings. When an e-mail address policy is modified and saved, all associated recipients are updated with the change. In addition, if a recipient object is modified, that recipient's e-mail address policy membership is reevaluated and enforced.  It is recommended that you use e-mail address policies in Exchange 2013 the way they were designed, as only the objects within the scope of the policy are affected by changes and the previous scalability and recipient update service issues no longer apply. Using a policy will ensure consistency for all mailboxes within a tenant.  One-off address can still be added to users individually using supported cmdlets. |
| Unsupported Solutions |  |
| Additional Comments | Understanding E-Mail Address Policies - <http://technet.microsoft.com/en-us/library/bb232171> |

### Transport

The underlying transport system used by Exchange relies in many ways upon certain assumptions, just like the other components discussed in this document. When attempting to configure Exchange to behave as a multi-tenant system some of those base assumptions must be understood and configuration changes made to work around them, or settings put in place that work equally well for all users on the system.

This section describes the challenges in transport that need to be solved to enable a hoster to use Exchange in a multi-tenant configuration.

|  |  |
| --- | --- |
| Problem or Issue Description | Preventing users sending emails to distribution groups owned by other tenants. |
| Recommended Approach | Restricting the senders that are allowed to send to a DG, and enforcing authentication for users sending to the DG. Both should be set using EAC or the Set-DistributionGroup cmdlet. |
| Unsupported Solutions | Directly editing or setting any DG properties in Active Directory and not using the built in tools. |
| Additional Comments | The default message delivery restrictions configured when a new distribution group allow All senders to send to the DG, but require that all senders be authenticated. Authenticated means any user on the system, which means any user from any tenant.  These defaults should be changed for every distribution group created. Each tenant organization usually contains at least one DG, and this is the object (or collection of objects if more than one DL is required) to use to restrict senders to being a member of. With this configuration, and with the requirement of only authenticated users being allowed to use the DG, senders will be adequately controlled.  Configure Message Delivery Restrictions - <http://technet.microsoft.com/en-us/library/bb397214.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Message size restrictions. |
| Recommended Approach | Generally speaking, you should set more restrictive limits at the points where messages enter your infrastructure. For example, any message size restrictions on your Edge Transport server receive connectors that receive messages from the Internet should be less than or equal to the message size restrictions you configure for your internal Exchange organization. It would be a waste of system resources for the Edge Transport server to accept and process a message from the Internet that would be rejected by your Mailbox servers. Make sure that your organization, server, and connector limits are configured in a way that minimizes any unnecessary processing of messages.  One exception to this approach is the user limits. User level limits take precedence over other message size restrictions. Therefore, you can configure a user to exceed the default message size limits for your organization. For example, you can allow a specific group of user mailboxes to send larger messages than the rest of the organization by configuring custom send and receive limits for those users.  Setting those limits would typically be accomplished at provisioning time based on service plan or service. |
| Unsupported Solutions | Any attempts to override or manipulate size limits in any way by not using options that are normally available using the built-in cmdlets available in the Exchange Management Shell or the Exchange Administration Center will be unsupported |
| Additional Comments | You can apply message size limits to individual messages that move through the Microsoft Exchange Server 2013 organization. You can restrict the total size of a message or the size of the individual components of a message, such as the message header, the message attachments, and the number of recipients. You can apply limits globally for the whole Exchange 2013 organization, or specifically for a particular connector or user object.  Understanding Message Size Limits - <http://technet.microsoft.com/en-us/library/bb124345.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | The postmaster address shown on non-delivery reports (NDR) and Delivery Status Notifications (DSN’s) is system wide. |
| Recommended Approach | It is recommended you configure a generic SMTP address to use as the postmaster address. This address should result in delivery to your helpdesk or service desk. |
| Unsupported Solutions |  |
| Additional Comments | Configure the External Postmaster Address using Set-TransportConfig - <http://technet.microsoft.com/en-us/library/bb124151> |

|  |  |
| --- | --- |
| Problem or Issue Description | Preventing name resolution of recipients and matching to directory entries from taking place when emails are sent between tenants. |
| Recommended Approach | Exchange Server 2013 CU1 ships with a feature that you can use to configure transport in such a way as to respect Address Book Policies.  When the Address Book Policy Routing Agent is installed and enabled following the published guidelines, and the *AddressBookPolicyRoutingEnabled* parameter of the **Set-TransportConfig** cmdlet is set to *True*, the agent will ensure messages sent between recipients with ABP’s are correctly resolved and appear as unresolved Exchange objects where appropriate. |
| Unsupported Solutions | Any transport agent based solution that does not follow the guidelines provided at <http://msdn.microsoft.com/en-us/library/dd877026(v=EXCHG.140).aspx> |
| Additional Comments | Install and Configure the Address Book Policy Routing Agent - <http://go.microsoft.com/fwlink/?LinkID=278861> |

|  |  |
| --- | --- |
| Problem or Issue Description | Routing of e-mail for tenants who have been migrated off the system.  The default behavior of Exchange is to resolve mail sent internally between recipients to their corresponding directory objects.  If the sender’s mailbox is subsequently removed, any attempt to reply will show the sender an unresolved *LegacyExchangeDN* in the to: field of the e-mail, perhaps a MailTip (if enabled) stating that the recipient address is invalid, or will result in an NDR.  If the original sender’s entire tenant is removed, any replied to emails would fail to route outside the system, as the original senders were considered internal, though in a different tenant. |
| Recommended Approach | Exchange Server 2013 CU1 ships with a feature that you can use to configure transport in such a way as to respect Address Book Policies.  When the Address Book Policy Routing Agent is installed and enabled following the published guidelines, and the *AddressBookPolicyRoutingEnabled* parameter of the **Set-TransportConfig** cmdlet is set to *True*, the agent will ensure messages sent between recipients with ABP’s are correctly resolved and appear as unresolved SMTP objects where appropriate.  This feature also ensures that replies to messages that appear to the client as unresolved SMTP objects, but were in fact Mailbox objects inside another tenant, and now exist as Contact objects inside another tenant are routed correctly. |
| Unsupported Solutions |  |
| Additional Comments | Messages which were delivered to users prior to deployment of Exchange Server 2013 CU1 (and subsequent enabling of AddressBookPolicyRoutingEnabled) will not be impacted by the new routing behavior, therefore resolved sender and recipient addresses within messages migrated from prior versions may still result in invalid recipient errors or NDRs due to unresolved LegacyExchangeDN values.  Install and Configure the Address Book Policy Routing Agent - <http://go.microsoft.com/fwlink/?LinkID=278861> |

|  |  |
| --- | --- |
| Problem or Issue Description | The *TLSReceiveDomainSecureList* and *TLSSendDomainSecureList* settings can only be configured at the Exchange Organization level. |
| Recommended Approach | If you choose to offer these features to your tenants, you should manage these lists for all tenants and ensure tenant users understand why the domain secure flag might be shown on some messages they receive. |
| Unsupported Solutions |  |
| Additional Comments | Using Domain Security: Configuring Mutual TLS - <http://technet.microsoft.com/en-us/library/bb123543.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Read Tracking can only be enabled or disabled at the Exchange Organizational level.  The *ReadTrackingEnabled* parameter in the Set-OrganizationConfig cmdlet specifies whether the tracking for read status for messages in an organization is enabled. The default value is *$false*. |
| Recommended Approach | If you choose to offer this feature to your tenants you should enable it at the organizational level.  If you want to allow the feature but prevent read receipts being delivered between tenants, this can be accomplished with a transport rule. |
| Unsupported Solutions |  |
| Additional Comments | Set-OrganizationConfig - <http://technet.microsoft.com/en-us/library/aa997443.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Scanning for viruses and spam. |
| Recommended Approach | It is recommended that you adopt a defense in depth strategy, combining cloud based anti-virus and anti-spam as well using the built-in transport based anti-virus agents on your mailbox servers to ensure mail sent between tenants is scanned. |
| Unsupported Solutions |  |
| Additional Comments | Enable the Anti-spam Agents on the Mailbox Server - <http://technet.microsoft.com/en-us/library/bb201691.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Message tracking logs are system wide. |
| Recommended Approach | In a multi-tenant configuration using Exchange 2013 we recommend you do not allow tenant administrators direct access to message tracking logs as it will expose data from all tenants.  You may decide to completely disable message tracking or you may choose to provide access to message tracking information via a custom interface or by some form of service request. |
| Unsupported Solutions |  |
| Additional Comments | Track Messages with Delivery Reports - <http://technet.microsoft.com/en-us/library/jj150554.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Outlook Protection Rules may expose tenant data |
| Recommended Approach | In a multi-tenant configuration using Exchange 2013 we recommend you do not configure any Outlook Protection Rules as it will expose SMTP domains from all tenants when Outlook Advanced Logging is enabled. |
| Unsupported Solutions |  |
| Additional Comments | If Outlook Protection Rules are enabled, all accepted domains are returned to the advanced logging file as part of the Outlook Protection Rules feature. If you do not use the feature, you should ensure the feature is not enabled.  Outlook Protection Rules - <http://technet.microsoft.com/en-us/library/dd638196.aspx> |

### Features and functionality

Exchange Server is a feature rich platform and was designed to enable users to closely collaborate together and therefore asserts some degree of trust common to all users on the system. Many of the features in Exchange were not designed with multiple tenants in mind, and so some features should either be configured in a specific way, or disabled altogether.

|  |  |
| --- | --- |
| Problem or Issue Description | Some EAC/ECP features will not work correctly in a multi-tenant configuration when using Exchange 2013.  For example, the distribution group self-service functionality can expose data from other tenants.  For example, adding a user to any RBAC group that exposes the Distribution Group Management options in ECP will likely result in exposing data from all tenants. |
| Recommended Approach to Solve | It is recommended that you disable the features that do not work correctly. For the DG self-service and management tools, you can do this by simply not including users in the ***MyDistributionGroupMembership*** RBAC role group that enables the functionality and user interface.  It is also recommended to completely disable access to the Exchange Administration Center by modifying the **Set-ECPVirtualDirectory –AdminEnabled** parameter on all tenant-facing servers. |
| Unsupported Solutions | Modification of any of the files that are used for EAC/ECP is unsupported. If you decide to build a control panel solution, that solution must only use built-in cmdlets and interfaces. |
| Additional Comments | Understanding Role Based Access Control - <http://technet.microsoft.com/en-us/library/dd298183.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Internal Out Of Office (OOF) messages are delivered between tenants.  Since Exchange Server 2007, a user has been able to set both an internal and an external OOF, and have Exchange deliver the OOF based on the sender being inside or outside the same Exchange Organization. In a multi-tenant configuration of Exchange such as that described in this document, all users in all tenants are considered internal to each other, and so the Internal OOF is sent between them if emails are exchange and OOF is set on a mailbox. |
| Recommended Approach | OOF messages are a specific message class, IPM.Note.Rules.Oof.Template.Microsoft, and therefore can be identified easily within transport.  There are several ways to solve this problem, depending on the features you want to offer to your tenants.  The simplest solution is to create a simple transport rule that deletes OOF messages to users when the recipient is also inside the organization. This will however also delete all OOF messages between users, even within the same tenant.  A more performance impacting solution would be to create multiple transport rules using groups to control the deletion of the OOF messages. Again, this means no OOF messages are delivered between tenants on the same system.  Another alternative is to write a custom transport agent to perform this action, perhaps examining the SMTP domains for both sender and recipient and taking appropriate action. |
| Unsupported Solutions | Any transport rules not built using the cmdlets or tools provided will be unsupported.  Any transport agent solution will be unsupported if it does not follow the guidelines provided at <http://msdn.microsoft.com/en-us/library/dd877026(v=EXCHG.140).aspx> |
| Additional Comments | Transport Rules - <http://technet.microsoft.com/en-us/library/dd351127> |

|  |  |
| --- | --- |
| Problem or Issue Description | Remote domain settings apply to all tenants. |
| Recommended Approach | It is recommended you only configure settings for remote domains which are acceptable to all tenants. Any settings you configure for a remote domain will be equally applied to all tenants configured on your solution. |
| Unsupported Solutions | Any attempt to override the default behavior using any methods other than the built-in tools would be unsupported. |
| Additional Comments | Understanding Remote Domains - <http://technet.microsoft.com/en-us/library/aa996309> |

|  |  |
| --- | --- |
| Problem or Issue Description | MailTips are shown for users in different tenants, or show inaccurate numbers for distribution groups.  MailTips do not respect hoster configured tenant boundaries. |
| Recommended Approach | In a multi-tenant configuration using the Exchange 2013, we recommend you disable some MailTips features rather than risk exposing data between tenants.  For example, the *MailTipsMailboxSourcedTipsEnabled* setting is used to control the display of user-configured OOF messages before messages are sent. If a user has configured an internal and external OOF, the internal OOF would be displayed to a sender from another tenant, which risks exposing data that should not be seen outside the tenant boundary.  The *MailTipsExternalRecipientsTipsEnabled* setting determines if Outlook will show a warning when sending an email to recipients that are outside the Organization. When used in a multi-tenant configuration it considers domains for all tenants as internal, and so does not provide the expected user experience and will not produce the warning for messages being sent between tenants.  It is not possible to scope the MailTips feature to a subset of users within the entire organization.  If you disable any MailTips functionality you might also consider disabling Group Metrics generation to reduce the load on the OAB generation servers.  You can change MailTips settings by using the Set-OrganizationConfig cmdlet. |
| Unsupported Solutions | Any attempts to manipulate, change or otherwise override the configuration the built-in cmdlets provide will be unsupported. |
| Additional Comments | MailTips - <http://technet.microsoft.com/en-us/library/jj649091.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Information Rights Management may expose tenant data |
| Recommended Approach | In a multi-tenant configuration using Exchange 2013 we recommend you do not configure IRM using AD Rights Management Server as it is not possible to create templates visible to only one subset of users.  In addition, as there is only one Exchange Organization all the keys are in some way related to each other and so there is very little real security at the level required for a feature like this to be defensible. |
| Unsupported Solutions |  |
| Additional Comments | Information Rights Management - <http://technet.microsoft.com/en-us/library/dd638140.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Data Loss Prevention (DLP) may expose tenant data |
| Recommended Approach | In a multi-tenant configuration using Exchange 2013 we recommend you plan and test any DLP features carefully before deciding to offer them to your tenants.  DLP policies can be a very powerful tool to prevent data loss, but the default options do not necessarily work when Exchange is configured in a multi-tenant way. The concepts of internal/external do not apply in the same way as they would in an on-premises deployment for example. |
| Unsupported Solutions |  |
| Additional Comments | Data Loss Prevention - <http://technet.microsoft.com/en-us/library/jj150527.aspx> |

### Design and Architecture considerations

The design decisions you make before you build your hosting system may differ than those you would make when designing for a typical Exchange 2013 deployment. In order to build a platform for a hosting deployment you should consider the issues in the following section at a minimum.

|  |  |
| --- | --- |
| Problem or Issue Description | You want a reference architecture document describing exactly what you need to build to hosted Exchange Server 2013 solution. |
| Recommended Approach | There are no plans at the time of writing to produce reference architectures for this type of solution.  It is recommended you review all the available materials to help you plan your deployment - <http://technet.microsoft.com/en-us/library/aa998636(v=exchg.150)> is a good starting point for Exchange Server 2013.  In addition, it is recommended you review the information published on the Exchange team’s blog site, as it contains additional useful articles which will help with your planning efforts. The blog is available at <http://blogs.technet.com/b/exchange/> |
| Unsupported Solutions |  |
| Additional Comments | Before installing Exchange 2013 for the first time, we recommend that you install it in an isolated test environment. Doing so can help reduce the risk of end-user downtime and negative ramifications to the production environment.  The test environment will act as a “proof of concept” for your new Exchange 2013 design and make it possible to move forward or roll back any implementations before deploying your production environments. Having an exclusive test environment for validation and testing allows you to perform pre-installation checks for your future production environments. By installing Exchange 2013 first in a test environment, we believe that your organization will have a better likelihood of success in a full production implementation.  The Test System should at the very least be used to fulfill the following:     * New software should be tested here to ensure it interoperates with other subsystems * All software updates, including security updates, should be tested here by running a standard full system test suite * The Test System should also be used to reproduce problems reported in production. In this way, debugging can be performed without impacting users, workarounds can be tested, and further troubleshooting performed. Once a fix is available, it can be tested to prove the problem has been solved * The Test System should contain working version of all related dependent systems, provisioning and billing for example. |

|  |  |
| --- | --- |
| Problem or Issue Description | When configuring External URLs and host names for OWA, EWS and Outlook Anywhere, what names should be used? |
| Recommended Approach | The URLs and hostnames configured returned to clients are the same across the system. It is not possible to configure tenant specific URLs to be returned via AutoDiscover. The recommendation therefore is to create generic and non-specific names that do not identify any specific tenants.  It is still possible to provide tenants with URLs that match their domain names for services such as OWA or ActiveSync (if they choose to manually configure their device), if that name is also added to the certificate, though it is not generally recommended for security and privacy reasons.  In this scenario, users can manually enter the URL and end up at the hosters’ site. For example, mail.contoso.com could be added to the certificate used by the hoster. If a user types in *https://mail.yourcompany.com/owa* or *https://mail.contoso.com/owa* they end up at the same site. However, this does result in the names being exposed on the certificate, and anyone viewing the certificate can see those names.  Another option might be to create tenant specific subdomains of one specific hosting domain, which also provides the benefit of allowing you to use wildcard certificates. For example, you obtain a certificate for *\*.yourhostingdomain.com* and create a subdomain for each tenant who requires a vanity domain, *contoso.yourhostingdomain.com* for example. You do not need to add names to the certificate and they can use their tenant specific sub-domain names. |
| Unsupported Solutions | It is not supported to modify or otherwise change the AutoDiscover XML response returned to the client in any way for any reason. |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Designing to future proof migrations.  How can you design the system to make future migrations easier? |
| Recommended Approach | Migration is always complex, and migration between different forests is even more so.  We recommend you think about decisions you can make which will make future migrations easier, even if they result in some upfront cost or time. Here are two examples;  Don’t allow your tenants to have non-expiring passwords - it might make your solution less user friendly if your tenants use clients that don’t make for easy password changes (POP/IMAP for example), but if there is a way for password changes via their client then not only do you make their accounts more secure, you also make future migrations simpler.  If you plan to migrate mailboxes between two forests you need some kind of directory and password synchronization solution in place. If you use a password synchronization solution such as the Microsoft Password Change Notification Service (PCNS) you can only replicate passwords when they are changed. If tenants never change their passwords, you cannot synchronize them to the new forest. That will result in a painful dual password experience at some point in the future.  It may seem easy to ask your customers to deploy XML files to their machines to force their client computers to reach the AutoDiscover endpoint you want them to use, and may seem necessary during a period of co-existence as mailboxes are moved between systems, but it rarely is required long term, and if left behind it results in problems when either the hoster changes something in their environment, or the user buys a new machine, or you want to migrate them to a newer version of your service.  Thinking through some of these scenarios early in the design process for the system you are building can help avoid problems down the road. If your service becomes large and your customer base is widely distributed, relying on client side actions to ensure your upgrade or migration works is risky. |
| Unsupported Solutions |  |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Writing applications to integrate with multi-tenant Exchange. |
| Recommended Approach | We recommend if you intend writing applications to provide extra features of functionality that you follow published guidance at all times, rely on services such as AutoDiscover for endpoint discovery, and use standard EWS APIs which will inherit features such as ABPs. |
| Unsupported Solutions | Any solutions that are not developed using publicized or documented APIs or interfaces will not be supported. |
| Additional Comments | Exchange Developer Center - <http://msdn.microsoft.com/en-us/exchange/default.aspx> and <http://msdn.microsoft.com/en-us/library/jj162981.aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Virtualizing your multi-tenant deployment |
| Recommended Approach | Virtualization is a supported option, as long as it conforms to our support statement and best practices guidance.    Don’t forget that there will be various tradeoffs associated with virtualization, and the overall cost of the deployment may be higher as a result of using virtualization when considering storage, monitoring, operations, server and hypervisor licenses, and various other operational expenses when compared with an optimized and cost-efficient non-virtualized system.    We recommend deploying a system that meets customer requirements, provides optimal performance, ensures high availability, and provides large mailboxes at low cost. If virtualization helps, then it should certainly be considered, but it should be carefully weighed against other options, as in our experience, large scale deployments of Exchange 2013 can often be built for a significantly lower cost (both in terms of CAPEX and OPEX) when deployed on physical hardware. |
| Unsupported Solutions |  |
| Additional Comments | Exchange 2013 Virtualization - <http://technet.microsoft.com/en-us/library/jj619301(EXCHG.150).aspx> |

### Scalability

Like any software, Exchange Server has limits in code, in performance, or in scale. Some of these limits are easy to identify, they exist in code and the code itself imposes the constraint. Some, such as performance and scale are much harder to define, as they depend upon the configuration and usage patterns of the system.

It is very possible that limits exist in components either listed, or not listed in this document, and that those limits will cause some scalability bottleneck or issue at some point. If you suspect you are hitting a hard limit on a type of object, you will need to gather solid data to support that conclusion and provide it to Microsoft. If you are experiencing generic performance and scalability limitations, it may not be possible to point to one specific component as it may be a combination of factors that led to the limit.

You should understand that it may not be possible to solve all the scalability limits of the product.

This section highlights known scalability limits, constraints, and considerations and makes recommendations based on existing understanding of the product.

|  |  |
| --- | --- |
| Problem or Issue Description | Ensuring one tenant cannot consume a disproportional amount of system resources, overloading the system, and negatively impacting the service as a whole. |
| Recommended Approach | It is recommended that you configure throttling policies per tenant, per your own defined service plan, or per user, depending upon your requirements.  When an Exchange organization is created, a default throttling policy is automatically created that implicitly governs all users within that organization. Although the default client throttling policy is generally sufficient to manage the load placed on your Exchange system, you may need to customize the default policy or add additional policies based on the needs of your deployment.  When hosting multiple tenants in your Exchange organization, you should define an acceptable load for each user of a tenant and assign the policy to the users during account creation.  You may also consider enabling network level throttling or quality of service between clients and Exchange if you feel it necessary. |
| Unsupported Solutions | Any other method of throttling usage would be unsupported. This includes throttling the network between servers, whether this is via hardware or software. |
| Additional Comments | Through policies, Exchange evaluates how each user uses the system and ensures that the resulting per-user load falls within acceptable boundaries as defined by the user's policy. The client throttling system tracks system usage on a per-user basis and uses the throttling policy associated with that user to determine if throttling should occur.  In Exchange 2013 installations, there's a single default throttling policy called First Organization.  If the non-default policy is corrupt or missing, it will first fall back to the default throttling policy for the organization. If the default policy is corrupt, then it falls back to a special policy defined in code called the "fallback policy". Given that this policy is embedded in the Exchange assemblies, there is little chance that such a read will fail. The values of the fallback policy are the exact values that default policies are assigned when Exchange is first installed.  Exchange Workload Management - <http://technet.microsoft.com/en-us/library/jj150503> |

|  |  |
| --- | --- |
| Problem or Issue Description | There are many system objects in Exchange, or that Exchange depends upon which have limits of some kind. Understanding these limits enables you to determine how large your system can grow to, and when you should begin planning for another deployment. |
| Recommended Approach | It is recommended you follow the following guidelines at a minimum. This list is not exhaustive and does not contain every possible object that might be constrained, but instead it aims to cover the kind of objects your deployment will likely be dependent upon and that you should be aware of the limits of.  You should also review any sizing and scalability documentation published by Microsoft to determine if any other limits apply and might constrain your solution.   * **Overall number of objects (mailboxes, contacts, DLs, etc.) in the same Exchange system** - There is no hardcoded limit but Microsoft recommends keeping the directory information tree (DIT) below 300GB for disaster recovery purposes. * **Transport Rules** - Microsoft recommends not exceeding 20,000 rules. When hosting this limit could easy be reached as many small organizations may each require their own rules. * **Public Folders** – If you choose to provide public folders to your tenants you should create a top level folder for each tenant, and apply the appropriate security to ensure only the members of each tenant can access it. * **Global Address Lists** – With Exchange Server 2013 there is no longer a hard coded limit to the number of GAL objects you can create for users with mailboxes on Exchange 2013 mailbox servers if you have configured Active Directory to operate in Windows Server 2008 forest functional level. It is no longer necessary to run the makegallinked.exe tool or change the schema definition properties of the GlobalAddressList attribute in Active Directory to enable you to create more than 1000 GALs. Once you reach the default limit of the GlobalAddressList attribute (approximately 1250 with the Windows Server 2008 Active Directory schema) you will receive a warning that the GAL you are attempting to create will only be accessible by users with a mailbox on Exchange 2010 or 2013.     **NOTE**: It is not supported (nor is it necessary) to run the makegallinked.exe tool or change the schema definition properties of the *GlobalAddressList* attribute in Active Directory in a new Exchange Server 2013 installation, you simply need to ensure the Active Directory is operating at the correct forest functional level and you use only the 2010 versions of the New-GlobalAddressList cmdlet.  If you are upgrading an existing Exchange Server 2007 installation to 2013 and the change has already been made, you will be supported; however, no attempts should be made to revert the schema change to take advantage of the new functionality.   * **Address Lists** – There are no hard-coded limits to the number of address lists you can create on the system, but there is a limit to the combined number of address lists and GALs a mail enabled object can be a member of, which is approximately 1000. If you wish to add a support@yourcompany.com type account to your tenant’s GALs you will need to use multiple objects if you have more than 1000 tenants. * **Offline Address Books** – There are no hard coded limits to the number of OABs you can create. Microsoft recommends OABs not exceed 1GB in size, and that you do not distribute OABs via Public Folders (not possible in Exchange Server 2013, but possible with Exchange Server 2010) when hosting.   You should ensure automatic OAB generation is disabled on all Mailbox servers that could host the Organization Mailbox with the OrganizationCapabilityOABGen Persisted Capability. A nightly process by default will evaluate all OABs and update them if required. The load this places on the system is significant if you have a large number of OABs. It is recommended that you create a process that updates specific OABs when there is a known change (such as a mailbox being added to a tenant) rather than allow automatic OAB generation.  It is recommended that you not generate OABs for every tenant by default, but instead only for those tenants that have Outlook access within their service plan. A POP3/IMAP4/OWA only customer does not use an OAB, and the time taken generating one is therefore a waste of system resources. You will still need an OAB for each tenant, for inclusion in the ABP, so it is recommended that you create an empty OAB and include it in the tenant’s ABP.  You should also be aware of OAB disk requirements. OABs are generated on a Mailbox server that hosts the Organization Mailbox with the OrganizationCapabilityOABGen Persisted Capability and kept on disk. A large number of OABs will consume a large amount of disk space, and if that mailbox is in a database protected by a DAG, the same disk space will be taken by any server in that DAG when the mailbox database becomes active.   * **Address Book Policies** – There are no hard coded limits to the number of ABP objects that can be created on the system. * **OWA Mailbox policies** - There are no hard coded limits to the number of OWA Mailbox Policy objects that can be created on the system. * **EAS Policies** - There are no hard coded limits to the number of Exchange ActiveSync Policy objects that can be created on the system. * **Accepted Domains** - There are no hard coded limits to the number of Accepted Domain objects that can be created on the system though large numbers of Accepted Domains can cause significant load on the system and should be used cautiously in large multi-tenant environments. Microsoft recommends not exceeding 150,000 accepted domains per forest. * **Remote Domains** – There are no hard coded limits to the number of Remote Domain objects that can be created on the system. * **Journal Rules** – There are no hard coded limits to the number of Journal rule objects that can be created on the system though journal rules can place a significant load on the system and should be used cautiously in large multi-tenant environments. * **UM Dial Plans** – There are no hard coded limits to the number of UM Dial Plan objects that can be created on the system. * **Databases** – The maximum supported size is approximately 16 TB, however our best practice is to keep databases at 200GB or less if they are standalone copies (i.e. not protected by a DAG) or if they are DAG protected the maximum recommended size is 2 TB. * **Servers** – There is a maximum of 65,000 servers in an Exchange organization. * **Message Classifications** – There are no hard coded limits to the number of Message Classification objects that can be created on the system. * **E-mail Address Policies** – There are no hard coded limits to the number of E-mail Address Policy objects that can be created on the system. * **Dynamic Distribution Groups** – There is a limit of 300,000 members in any one dynamic distribution group though we recommend you not attempt to create groups this large unless you understand the impact and load it places on your system. * **UM Auto Attendants** – There are no hard coded limits to the number of UM Auto Attendant objects that can be created on the system. * **UM Mailbox Policies** – There are no hard coded limits to the number of UM Mailbox Policy objects that can be created on the system. |
| Unsupported Solutions | As discussed previously, it is not supported (nor is it necessary) to run the makegallinked.exe tool or change the schema definition properties of the GlobalAddressList attribute in Active Directory in a new Exchange Server 2013 installation. If you are upgrading an existing Exchange Server 2007 installation to 2013 and the change has already been made, you will be supported. No attempts should be made to undo the previous change to take advantage of the new functionality.  It is unsupported to exceed any limits where specifically stated in this section. |
| Additional Comments |  |

|  |  |
| --- | --- |
| Problem or Issue Description | Configuring AutoDiscover, Outlook Anywhere and OAB web sites in a multi-tenant configuration. |
| Recommended Approach | You should either use SRV records or create an additional web site on each CAS for initial client AutoDiscover requests, in order to allow client to be redirected to your AutoDiscover service, negating the need to put every tenant’s name on your SSL certificate.  The process is documented here - <http://technet.microsoft.com/en-us/library/ff923256.aspx> |
| Unsupported Solutions | It is not supported to run more than one instance of the rpcproxy.dll on a server, nor is it supported to move the rpcproxy.dll to a web site other than the default website. |
| Additional Comments | Additional information about AutoDiscover is in the Exchange 2007 AutoDiscover Service White Paper - <http://technet.microsoft.com/en-us/library/bb332063(EXCHG.80).aspx> |

|  |  |
| --- | --- |
| Problem or Issue Description | Managing large static or dynamic distribution groups. |
| Recommended Approach | It is not generally recommended to use dedicated DG expansion servers as they become a single point of failure and if dedicated servers are unavailable, they can cause service outages.  It is recommended that you size your deployment so that large DG expansion is factored in if you expect it to be a frequent occurrence. |
| Unsupported Solutions |  |
| Additional Comments |  |

## Migration From Other Exchange Hosting Solutions

Microsoft has created documentation to assist in the migration from Exchange 2010 /Hosting mode or HMC to Exchange Server 2010 Service Pack 2. Microsoft does not plan to update this guidance for Exchange Server 2013, though much of the same content applies.

### Exchange 2010 /Hosting to Exchange 2010

This document is available at the following location:

<http://go.microsoft.com/fwlink/?LinkId=242017>

### HMC to Exchange Server 2010

This document is available at the following location:

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=28714>

## Multi-Tenant Scale Guidance

This guidance document for Exchange Server 2010 is available at the following location: <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=28565>

The guidance document for Exchange Server 2013 will be published later in 2013.

## Appendix

## Legal Notice

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Mobile, Windows Server, Active Directory, ActiveSync, Forefront, Outlook, and SharePoint are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.