Petri
IT Knowledgebase

10 Featured Articles Serving IT Professionals in their Workplace

Exclusively Published on Petri.com

Contents

Petri

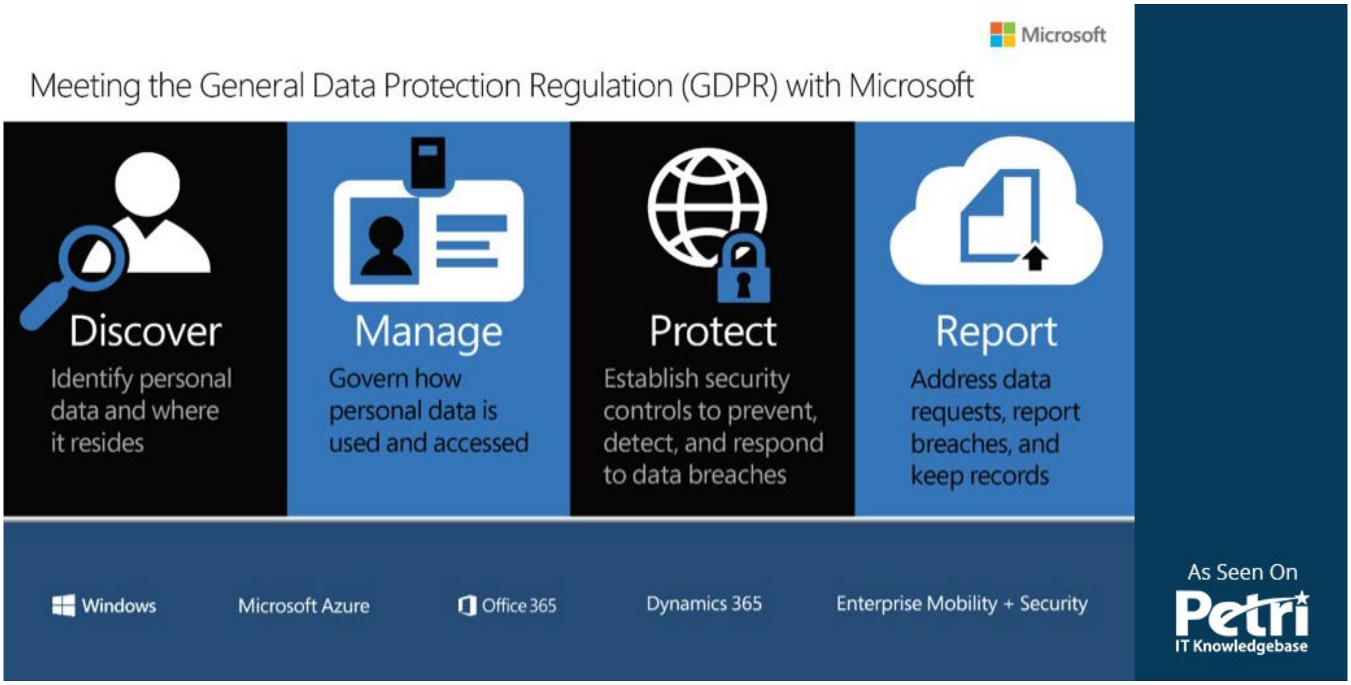
IT Knowledgebase

Featured Articles from Petri.com

Petri.com serves IT Professionals by providing original content that helps them solve problems, do their jobs more effectively and advance their careers.

What GDPR means to Office 365

Published on Petri.com August 17, 2017 by Tony Redmond


Microsoft
Meeting the General Data Protection Regulation (GDPR) with Microsoft
Discover
Identify personal data and where it resides
Manage
Govern how personal data is used and accessed
Protect
Establish security controls to prevent, detect, and respond to data breaches
Report
Address data requests, report breaches, and keep records
Windows
Microsoft Azure
Office 365
Dynamics 365
Enterprise Mobility + Security
As Seen On
Petri
IT Knowledgebase

GDPR Affects All European Businesses

From May 25, 2018, companies with business operations inside the European Union must follow the **General Data Protection Regulations**(GDPR) to safeguard how they process personal data "*wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*" The penalties set for breaches of GDPR can be up to 4% of a company's annual global turnover. For companies like Microsoft that have operations within the EU, making sure that IT systems do not contravene GDPR is critical. And as we saw on August 3, even the largest software operations like Office 365 **can have a data breach**.

Because many applications can store data that might come under the scope of GDPR, the regulation has a considerable influence over how tenants deal with personal data. The definition of personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

GDPR goes on to define processing of personal data to be "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*."

In effect, individuals have the right to ask companies to tell them what of their personal data a company holds, to correct errors in their personal data, or to erase that data completely. Companies need to know what personal data they hold, make sure that they obtain consents from people to store that data, protect the data, and notify authorities if data breaches occur.

On first reading, this might sound like what companies do – or at least try to do – today. The difference lies in the strength of the regulation and the weight of the penalties should anything go wrong. In other words, GDPR deserves your attention.

Putting GDPR into Context

The definitions used by GDPR are quite broad. To move from the theoretical to practicality, an organization needs to understand what personal data it holds for its business operations and where they use the data within software applications. However, it is easy to imagine examples of where personal information might be inside Office 365 applications, including:

- Annual reviews written about employees stored in a SharePoint or OneDrive for Business site.
- A list of applicants for a position in an Excel worksheet attached to an email message.
- Tables holding data (names, employee numbers, hire dates, salaries) about employees in SharePoint sites.

Other examples might include contract documentation, project files that includes someone's personal information, and so on.

Data Governance Helps

Fortunately, the work done inside Office 365 in the areas of data governance and compliance help tenants to satisfy the requirements of GDPR. These features include:

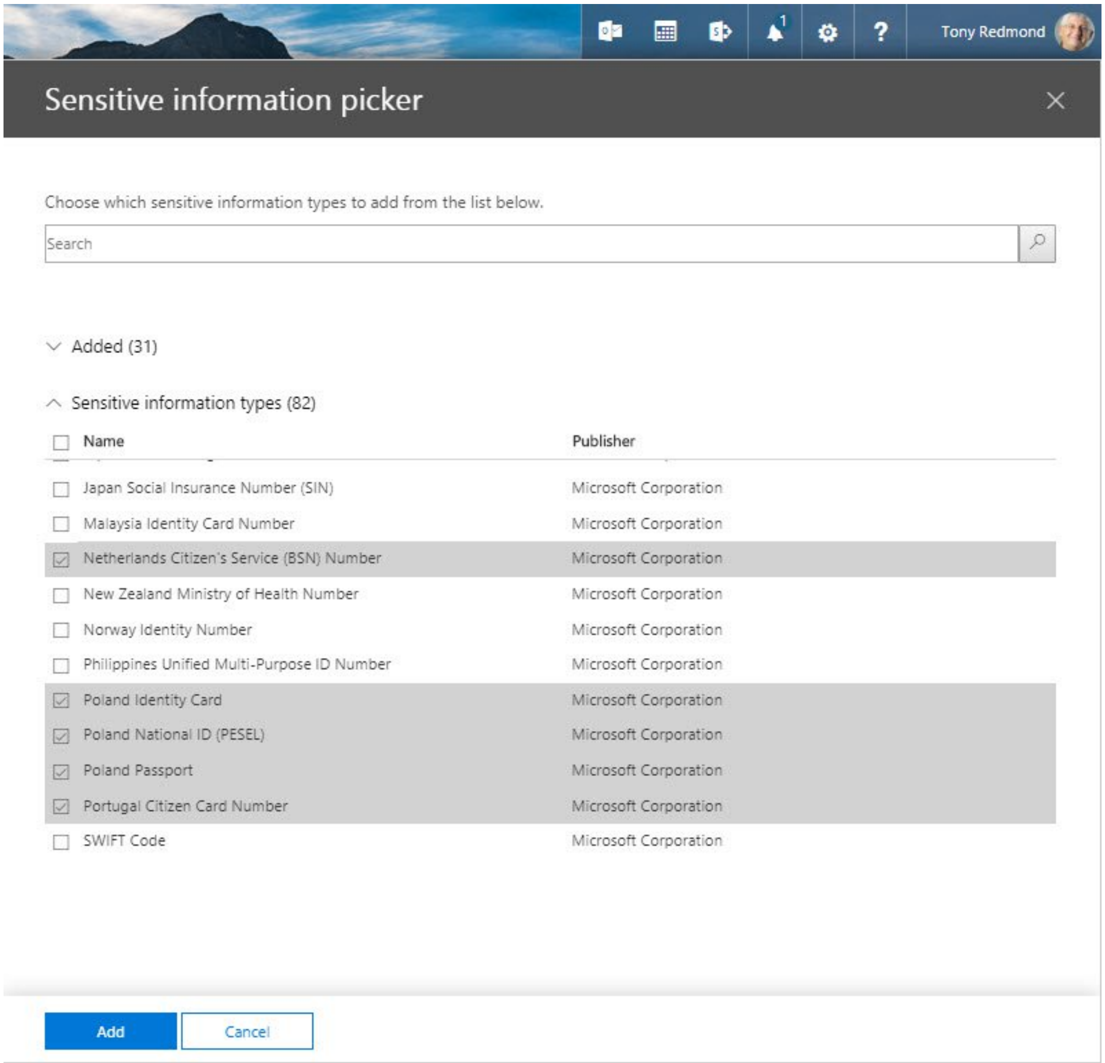
- Classification labels and policies to mark content that holds personal data.
- Auto-label policies to find and classify personal data as defined by GDPR. Retention processing can then remove items stamped with the GDPR label from mailboxes and sites after a defined period, perhaps after going through a manual disposition process.
- Content searches to find personal data marked as coming under the scope of GDPR.
- Alert policies to detect actions that might be violations of the GDPR such as someone downloading multiple documents over a brief period from a SharePoint site that holds confidential documentation.
- Searches of the Office 365 audit log to discover and report potential GDPR issues.
- Azure Information Protection labels to encrypt documents and spreadsheets holding personal data by applying RMS templates so that unauthorized parties cannot read the documents even if they leak outside the organization.

Let's explore some of the technology that exists today within Office 365 that can help with GDPR.

Using Classification Labels

As mentioned above, you can create a classification label to mark personal data coming under the scope of GDPR and then apply that label to relevant content. If you have Office 365 E5 licenses, you can create an auto-label policy to stamp the label on content in Exchange, SharePoint, and OneDrive for Business found because documents and messages hold sensitive data types known to Office 365.

Figure 1 shows how to select from the set of sensitive data types available in Office 365. The set is growing steadily as Microsoft adds new definitions. At the time of writing, 82 types were available, 31 of which are obvious candidates to use in a policy because they are for sensitive data types such as country-specific identity cards or passports.



Sensitive information picker

Choose which sensitive information types to add from the list below.

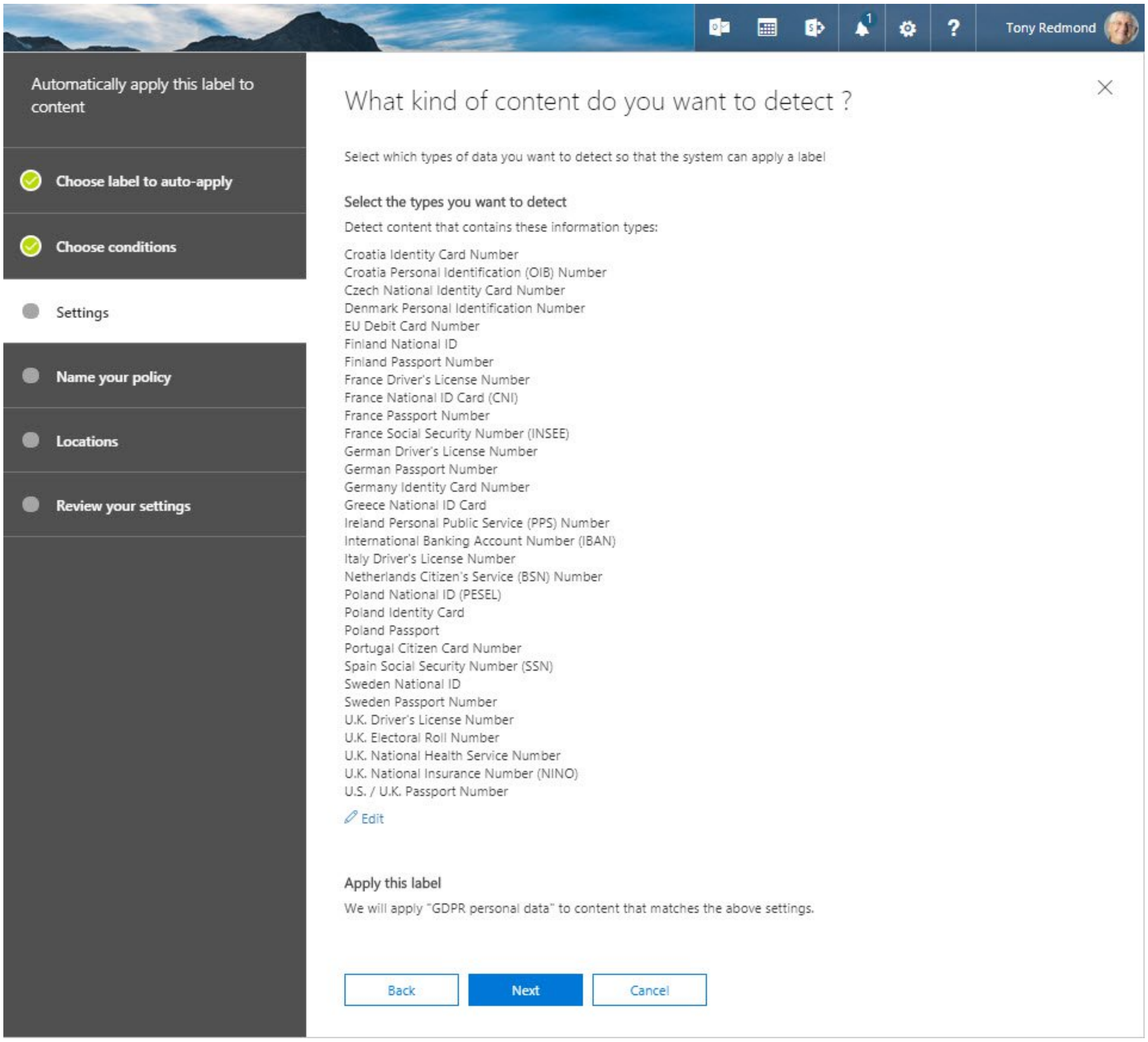
Added (31)

Sensitive information types (82)

	Name	Publisher
□	Japan Social Insurance Number (SIN)	Microsoft Corporation
□	Malaysia Identity Card Number	Microsoft Corporation
☑	Netherlands Citizen's Service (BSN) Number	Microsoft Corporation
□	New Zealand Ministry of Health Number	Microsoft Corporation
□	Norway Identity Number	Microsoft Corporation
□	Philippines Unified Multi-Purpose ID Number	Microsoft Corporation
☑	Poland Identity Card	Microsoft Corporation
☑	Poland National ID (PESEL)	Microsoft Corporation
☑	Poland Passport	Microsoft Corporation
☑	Portugal Citizen Card Number	Microsoft Corporation
□	SWIFT Code	Microsoft Corporation

Figure 1: Selecting personal data types for an auto-label policy (image credit: Tony Redmond)

Figure 2 shows the full set of sensitive data types that I selected for the policy. You can also see that the policy applies a label called "GDPR personal data" to any content found in the selected locations that matches any of the 31 data types. Auto-apply policies can cover all Exchange mailboxes and SharePoint and OneDrive for Business sites in a tenant – or a selected sub-set of these locations.



What kind of content do you want to detect ?

Select which types of data you want to detect so that the system can apply a label

Select the types you want to detect

Detect content that contains these information types:

Croatia Identity Card Number
Croatia Personal Identification (OIB) Number
Czech National Identity Card Number
Denmark Personal Identification Number
EU Debit Card Number
Finland National ID
Finland Passport Number
France Driver's License Number
France National ID Card (CNI)
France Passport Number
France Social Security Number (INSEE)
German Driver's License Number
German Passport Number
Germany Identity Card Number
Greece National ID Card
Ireland Personal Public Service (PPS) Number
International Banking Account Number (IBAN)
Italy Driver's License Number
Netherlands Citizen's Service (BSN) Number
Poland National ID (PESEL)
Poland Identity Card
Poland Passport
Portugal Citizen Card Number
Spain Social Security Number (SSN)
Sweden National ID
Sweden Passport Number
U.K. Driver's License Number
U.K. Electoral Roll Number
U.K. National Health Service Number
U.K. National Insurance Number (NINO)
U.S. / U.K. Passport Number

Apply this label

We will apply "GDPR personal data" to content that matches the above settings.

Figure 2: The full set of personal data types for a GDPR policy (image credit: Tony Redmond)

Using classification labels to mark GDPR content has another benefit in that you can search for this content using the *ComplianceTag* keyword (for instance, ComplianceTag:"GDPR personal data").

It can take up to a full week before auto-label policies apply to all locations. In addition, an auto-label policy will not overwrite a label that already exists on an item. These are small issues. The big problem here is that classification labels only cover some of Office 365. Some examples of popular applications where you cannot use labels are: Teams, Planner and Yammer.

Microsoft has plans to expand the Office 365 data governance framework to other locations (applications) over time. Given the interest in GDPR, hopefully some or all of the locations mentioned above will support data governance by May 2018.

Right of Erasure

Finding GDPR data solves one problem. A further challenge is posed by article 17 of GDPR (the "right of erasure"), which says: "*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay."* In other words, someone has the right to demand that an organization should erase any of their personal data that exists within the company's records. Content searches can find information about someone using their name, employee number, or other identifiers as search keywords, but erasing the information is something that probably needs manual processing to ensure that the tenant removes the right data and just that data.

You can find and then remove documents and other items holding someone's name or another identifier belonging to them using tools such as Exchange's venerable **Search-Mailbox cmdlet** or Office 365 content searches. However, if the data is on-hold because the company needs to keep items for regulatory or legal purposes, can you then go ahead and remove the items? Remember that the purpose of placing content on-hold is to ensure that no-one, including administrators, can remove that information from Exchange or SharePoint.

The GDPR requirement to erase data on request means that administrators might have to release holds placed on Exchange, SharePoint, and OneDrive for Business locations to remove the specified data. But once you release a hold, you weaken the argument that held data is immutable. The danger exists that background processes or users can then remove or edit previously-held data and so undermine a company's data governance strategy.

The strict reading of GDPR appears to leave no doubt that organizations must process requests to erase personal data upon request, unless it is needed to exercise or defend legal claims under article 17.3e. But what if the company needs to keep some of the data to satisfy regulations governing financial transactions or other interactions? This is not something that IT can solve. Lawyers will have to interpret requests and understand the consequences before making decisions and it is likely that judges will have to decide some test cases in different jurisdictions before full clarity exists.

Hybrid is More Difficult

No doubt exists that Microsoft is working to help Office 365 tenants with GDPR. However, not quite the same effort is going to help on-premises customers. Some documentation exists to deal with certain circumstances (like **how to remove messages held in Recoverable Items**), but the feeling I have picked up is that on-premises customers feel they have to figure things out for themselves.

In some respects, this is understandable. After all, every on-premises deployment is slightly different and exists inside specific IT environments. Compared to the certainty of Office 365, developing software for on-premises deployment must take the foibles of individual customers into account.

On-premises software is more flexible, but it is also more complicated. Developing solutions to help on-premises customers deal with GDPR might be more of a challenge than Microsoft wants to take on now, especially given their focus of moving everything to the cloud.

Solutions like auto-label; policies are unavailable for on-premises servers. Those running on-premises SharePoint and Exchange systems must therefore come up with their own ways to help the businesses that they serve deal with personal data in a manner that respects GDPR.

SharePoint Online GitHub Hub

If you work with SharePoint Online, you might be interested in the **SharePoint GDPR Activity Hub**. At present, work is only starting, but it is a nice way to share information and code with similarly-liked people.

ISV Initiatives

Every week I seem to receive an announcement about an ISV-sponsored white paper on GDPR and how their technology can help companies cope with the new regulations (here is **an example from Forcepoint**). There is no doubt that these white papers are valuable, if only for the introduction and commentary by experts that the papers usually feature. But before you resort to an expensive investment, ask yourself whether the functionality available in Office 365 is enough. If not, then look at the ISV offerings more closely.

Technology Only Part of the Solution

GDPR will affect Office 365 because it will make any organization operating in the European Union aware of new responsibilities to protect personal data. However, technology seldom solves problems on its own. The nature of regulations like GDPR is that training and preparation are as important if not more important than technology to ensure that users recognize and properly deal with personal data in their day-to-day activities. You can deploy Office 365 features to support users in their work, but do not expect Office 365 to be a silver bullet for GDPR.

Understanding Microsoft 365

Published on Petri.com November 3, 2017 by Aidan Finn

In this post, I'll discuss one of the hottest subjects that my customers want to learn more about; Microsoft 365.

Complete User Management

What is the function of It when it comes to enabling end users to contribute to the organization? Our job is to:

- Provide them with the tools that they require
- Aid employees as required
- Protect the assets of the company

All too often, IT departments view each component of each of those functions as different tools. That started to change with Office Servers. When we combined Active Directory with email (Exchange Server), we realized that we could have a smarter communications system that understood us and our intentions. Along came Lync Server and SharePoint server and we not only communicated, but we collaborated as dynamic teams, not just as loosely coupled co-workers.

In response to external threats, Microsoft created a cloud alternative to Office Servers called Office 365. This was a game changer – now we can all have the latest version of Exchange Online, SharePoint Online, Skype for Business, and many other features were added such as Teams, Office Groups, Flow, and the Office suite on our devices. By being in the cloud, we can access those services from anywhere, with the knowledge that the smartest IT security minds in the business are protecting our data while it is in the cloud.

But that was just one part of the toolset. There are other requirements, such as provisioning and protecting devices, and securing those devices. We have tools for that, but often those are traditional corporate tools. Many corporations and small businesses don't do the "corporate device" anymore, and end users are bringing their own laptops, phones and tablets to the office because those are the tools that work best for them. How do you provision such machines?

Threats have changed too. With mobility being a reality, users live outside of the edge firewall, not that blocking ports does much good anymore! We need a more intelligent protection of assets from today's form of attack: identity theft and zero-day malware.

Bringing Solutions Together

When addressing those needs, we've cobbled together an unconnected collection of tools. We've forgotten that Active Directory provided us with the glue for a smarter system. Users need simple solutions with easy-to-use security – easy for the user is best because resistance by users will kill security. When Active Directory is coupled (by Azure AD Connect) with Azure Active Directory (Azure AD), we can create a single identity across the organization, the management tools, and potentially 3,000 third-party cloud solutions come under the control of corporate governance & control.

All of Microsoft's cloud solutions are powered by Azure AD, and that means that a customer can have a single pane of glass for enabling users and securing company assets. Microsoft has been selling these tools for years, and adding to them with internal development and acquisitions. Quite honestly, some of these tools have been completely unknown to many Microsoft partners and customers because the Microsoft portfolio is huge. Microsoft realized this and decided to simplify things by offering two integrated bundles to customers under the banner of Microsoft 365.

Microsoft 365

The goal of Microsoft 365 is to bring together the following in an easy to understand and deploy package:

- Productivity (Office 365)
- Provisioning of devices
- Security

There are two versions of Microsoft 365 depending on the size or regulatory/business needs of the customer:

- **Microsoft 365 Business**: A plan based on Microsoft Office 365 Business Premium that is suitable for organizations up to 300 users.

- **Microsoft 365 Enterprise**: Based on Office 365 E3 and Office 365 E5, for larger organizations, and/or companies with specific regulatory requirements.

Microsoft 365 Business

If you work in the small/medium business sector, then this is the package that you will probably be interested in – you might opt for the Enterprise SKUs instead if you need some of the management/security/auditing/compliance features that it offers.

Office 365 Business Premium offers a large set of functionality, including Microsoft Office for PCs& Macs, phones, and tablets:

- Exchange Online with 50 GB mailboxes
- 1 TB of OneDrive for Business per user
- SharePoint
- Skype for Business
- Microsoft Teams
- Yammer

There are many more smaller services such as Planner or Booker that can add great value to a business.

But Office is just the start! With Microsoft 365 Business you also get:

- **Device management**: Single console user/device settings management, self-service PC configuration via AutoPilot, and automatic deployment of Microsoft Office to Windows 10 PCs. Note that this management is not Intune as has been commonly and incorrectly reported.
- **Security**: Centralized management of Defender on Windows 10, and the ability to secure company data across devices.

If you want security then you'll want the latest version of Windows. An upgrade to Windows 10 from Windows 7 or 8.1 Pro is included in Microsoft 365 Business.

Microsoft 365 Business is now available for companies with less than 300 users.

Microsoft 365 Enterprise

Being based on Office 365 E3 or E5, one can tell that Microsoft 365 Enterprise is intended for organizations that require more control and security. All of the features of Office 365 Business Premium are included, but one gets more, including:

- Office 365 Pro Plus
- Skype for Business Broadcast (10,000 attendees)
- eDiscovery & Legal Hold
- Classification, retention, and deletion policies.
- And more.

Note that the E5 SKU of Microsoft 365 Enterprise includes Office 365 E5. This adds:

- Power BI Pro
- Exchange Online Advanced Threat Protection (zero-day malware scanning)

- Office 365 Cloud App Security risk assessment
- A cloud-based PBX phone system

For management and security, Microsoft 365 Enterprise includes the Enterprise Mobility + Security (EMS) suite, with the E3 and E5 SKUs being available:

- **Intune**: Device management for PCs, phones, and tablets, software deployment, policy management, and secure selective wipe of personal devices.
- **Azure AD Premium**: Take control of identity across all services, enable multi-factor authentication, self-service password resets/group management, and much more.
- **Advanced Threat Analytics**: Detect unusual patterns of behaviour in your on-premises network.
- **Azure Information Protection**: Protect company data using templates/policy no matter where those documents go.
- **Cloud App Security (E5 only)**: Assess third party cloud service usage, and enforce data policies.

Security systems would be useless without a secure endpoint, so Microsoft includes Windows 10 Enterprise in this bundle. Windows 10 E3/E5 offer the best Defender features (build 1709) for protecting a company against attacks against today's entry point (the PC instead of the firewall), leveraging new pattern behaviour and AI-powered systems and hardware offloads to detect/contain threats against the business.

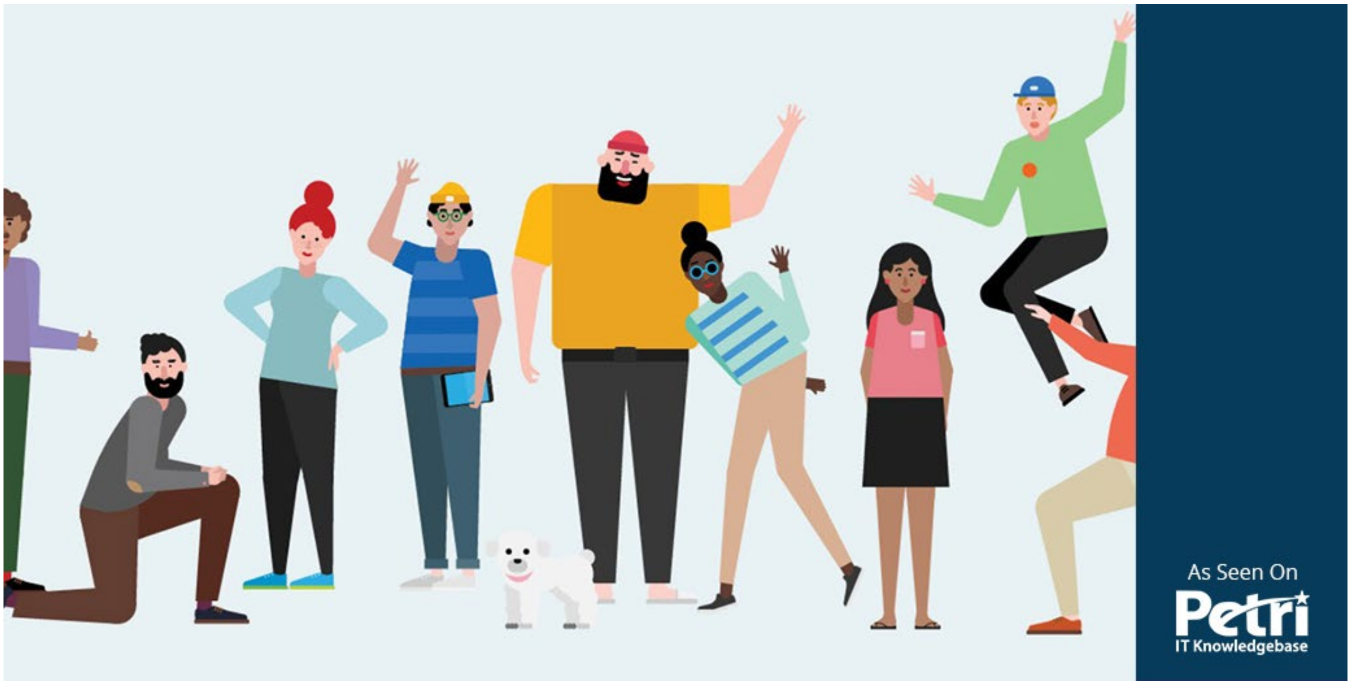
Microsoft 365 Enterprise is available today.

Opinion

From a customer's point of view, Microsoft 365 makes life easier. One bundle covers so many things and offers a lot of value. From a system integrator's/partner's point of view, they can have a single conversation with a customer to enable productivity and to protect the business. Not only that, but the customer is getting a lot of value for less than the sum of the total parts. Microsoft 365 offers an integrated solution to enable & protect employees and mobile company assets, that should provide 365-degree support against a new world of threats, that empowers the user instead of restricting them.

What You Need to Know about Teams and Office 365 Retention Policies

Published on Petri.com April 17, 2018 by Tony Redmond



Teams Becomes More Compliant

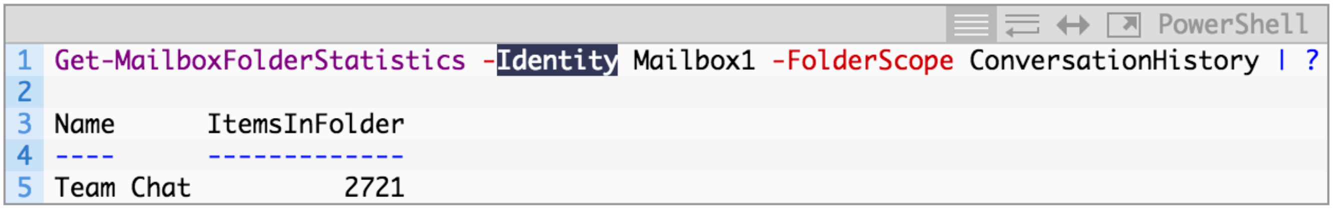
It's April, so it must be time for Microsoft to launch some new compliance features for Office 365. Last April, Microsoft launched the new **Office 365 data governance framework**, including retention policies and classification labels. Around the same time, Teams began to record **compliance records for personal and channel conversations** in user and group mailboxes. Now, to complete the circle, **Office 365 retention policies can process Teams compliance records**. All of which is good news with regulations like **GDPR on the near-term horizon**.

Office 365 retention policies support OneDrive for Business and SharePoint Online libraries, so it has always been possible to control some Teams content. The new initiative covers retention management for conversations, which exist in the Teams chat and media services running in Azure.

The MFA Helps with Compliance

Microsoft took an interesting approach to apply retention policies to conversations. Instead of building a new background process to interpret and execute the instructions as described in retention policies, Teams uses the Exchange Managed Folder Assistant (MFA) to process the compliance records held in user and group mailboxes.

As you might recall, each time someone posts a message to a channel, Teams captures a copy of the message in the Team Chat folder of the group mailbox belonging to the host team for the channel. Copies of messages sent to personal chats end up in the same folder in the mailboxes of participants. Office 365 indexes these compliance records to make them available for eDiscovery. To see how many Teams compliance records are in a (group or user) mailbox, use this PowerShell command:

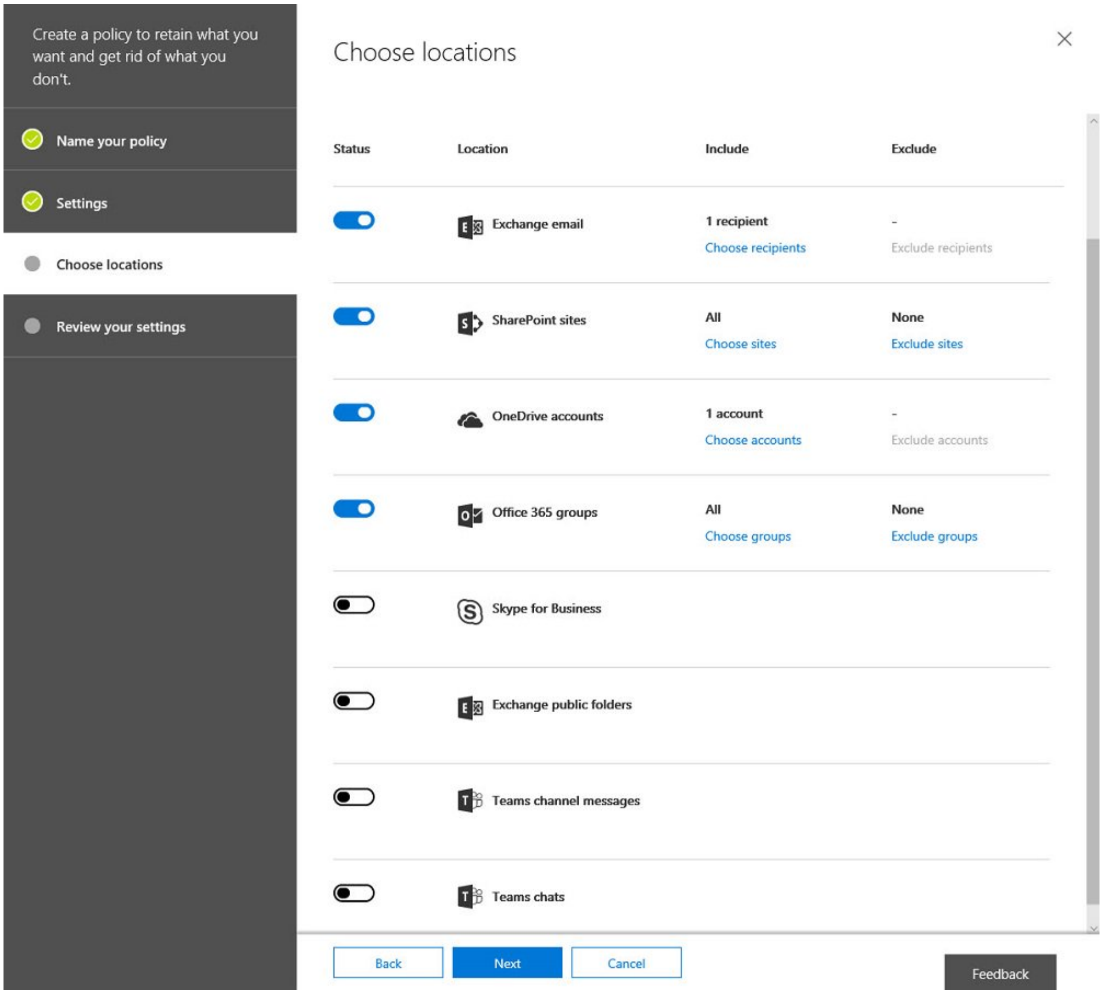


```
Get-MailboxFolderStatistics -Identity Mailbox1 -FolderScope ConversationHistory | ?

Name       ItemsInFolder
----       -------------
Team Chat           2721
```

The logic behind using MFA as the fulcrum for retention processing is impeccable. MFA already understands Exchange mailbox retention policies and Office 365 retention policies. It is a lot easier to include some processing in MFA for Teams compliance records than it is to write a new background agent specifically for Teams retention.

Retention for Teams

Apart from upgrading MFA, Office 365 needed two big updates to enable Teams retention. First, Office 365 retention policies now support *Teams channel messages*(in group mailboxes) and *Teams chats* (in user mailboxes) as processable locations (Figure 1).



Create a policy to retain what you want and get rid of what you don't.

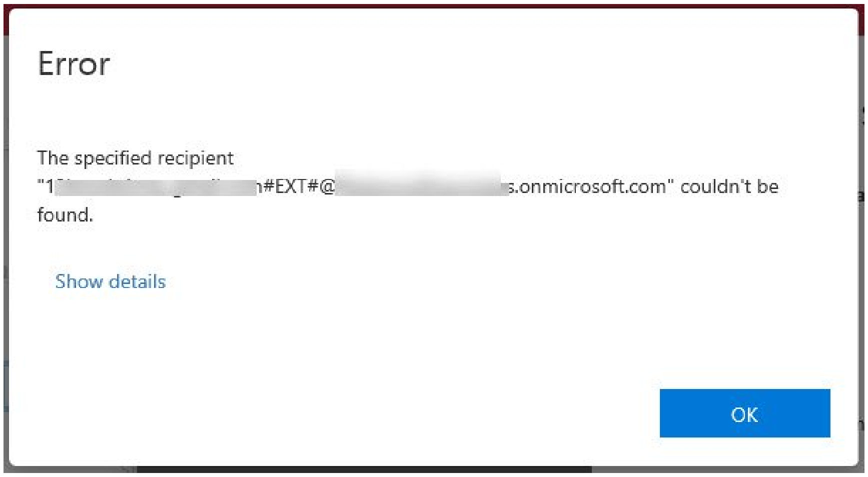
- ✓ Name your policy
- ✓ Settings
- ● Choose locations
- ● Review your settings

Choose locations

Status	Location	Include	Exclude
On	Exchange email	1 recipient Choose recipients	- Exclude recipients
On	SharePoint sites	All Choose sites	None Exclude sites
On	OneDrive accounts	1 account Choose accounts	- Exclude accounts
On	Office 365 groups	All Choose groups	None Exclude groups
Off	Skype for Business		
Off	Exchange public folders		
Off	Teams channel messages		
Off	Teams chats		

Figure 1: Teams shows up in retention policy locations (image credit: Tony Redmond)

In testing retention policies for Teams, I noticed some glitches of the type that you see when software is new. For example, you can select a guest user account and add it to a policy, even though these users don't have mailboxes. Thankfully, Office 365 checks users before creating the policy (Figure 2). On a more practical note, there's no support for bulk addition of users by adding a distribution group or Office 365 group to the policy.



Error

The specified recipient "1[redacted]#EXT#@[redacted]s.onmicrosoft.com" couldn't be found.

Figure 2: A guest user can't be found, so they can't be in a Teams retention policy (image credit: Tony Redmond)

You can add Teams to a policy that don't exist (because they are Office 365 Groups that are not enabled for Teams). Office 365 did not detect the presence of these groups and was happy to create the policy with them in it, possibly because they might be team-enabled in the future.

Types of Teams Retention

The new locations let administrators define a retention policy to remove Teams content after it reaches a certain age. For example, you might decide to remove all personal chats after six months while keeping channel messages for a year.

The separation between channel messages and personal chats exists because some tenants might want to impose different retention regimes on shared content (in channels) and personal content (in chats).

Some might, but I think most tenants will look to impose a common retention policy across both personal and channel chats, if only because personal chats often host the same kind of business- discussions that occur in the more formal setting of a channel. My experience of Teams is that a lot of sensitive work happens through personal chats, so it is reasonable to view these messages to be as important as those in the more formal context created by channels.

The norm for Teams is to keep messages forever. Apart from removing content after a set period, retention policies also allow tenants to make sure that Office 365 keeps content for as long as is necessary, which you might need to do to satisfy a government or industry regulation. In this case, as users do not have access to items in the hidden Teams Chat folder through clients like OWA and Outlook, it is unlikely that anyone will try to remove a Teams compliance record before its time, but if they do, Office 365 will keep a copy.

Substrate Processing

The second change is that Microsoft extended processing in the Office 365 substrate to synchronize the removal of any Teams compliance records by MFA back to the Teams chat service. Until now, Teams used the substrate to create compliance records in group or user mailboxes (and remove the items, if someone deletes a message in Teams), so the flow has been one-way.

When MFA removes Teams compliance records from mailboxes based on a policy setting (for instance, an item expires after six months), those removals ripple back through the substrate to Teams, which removes the items from the chat service. Eventually, as clients synchronize with Teams, the items disappear from local caches and the retention cycle completes.

Synchronization Takes Time

The time necessary for removed items to disappear completely from Office 365 varies according to when MFA processes a mailbox (the SLA for MFA to process all mailboxes in a tenant is a week), the synchronization between the substrate and Teams, and client synchronization with Teams. Other factors such as throttling of background processes due to user load also influence timing and while the clean-up occurs, it will still be possible for removed items to show up in content searches. Microsoft says that it could take up to 30 days for Teams to clean up content, but this period should be shorter.

A Separate Policy for Teams

Teams uses separate retention policies for chats, so you cannot include Teams processing in a retention policy that spans other workloads (and on a technical note, Teams retention policies use separate cmdlets: *New-TeamsRetentionCompliancePolicy* and *New-TeamsComplianceRetentionRuleTeams*). You can have one retention policy that applies to both personal and channel conversations, or one for each type – or indeed, multiple policies to process different sets of teams and users.

Using a separate retention policy for chats means that you need at least two retention policies to achieve full coverage of Teams content – one (or two) for chats, and the other for SharePoint and OneDrive. In addition, Teams does not support the removal of items less than 30 days old, so the smallest retention period is 30 days.

Teams does not support the advanced retention settings available in other workloads, such as the ability to search for specific items using keywords or to look for items that hold sensitive data. This functionality might come when Teams supports data loss prevention (DLP) policies, which is on the Office 365 roadmap.

If you want retention policies to apply to the content posted in the SharePoint document libraries used by Teams, you must include those sites in the SharePoint section of the retention policy. A retention policy cannot process data stored in other locations used by Teams such as third-party applications accessed through tabs or bots.

One Size Fits All Policy

Retention policies can do two things. You either keep content for at least the retention period or remove content after the retention period elapses. Teams supports either option, but what it does not do (at least today) is give users the ability to mark specific messages for longer- or shorter-term retention. SharePoint and Exchange support this kind of flexibility through classification labels or personal tags.

For instance, if you need to keep some content for ten years for audit purposes and the retention policy removes all items after six months, you can assign a personal tag or classification label to items in a mailbox or classification labels to documents in SharePoint or OneDrive for Business sites. Although Teams retention is based on the compliance records in user mailboxes, clients cannot access the Team Chats folder to apply retention tags to the items stored there.

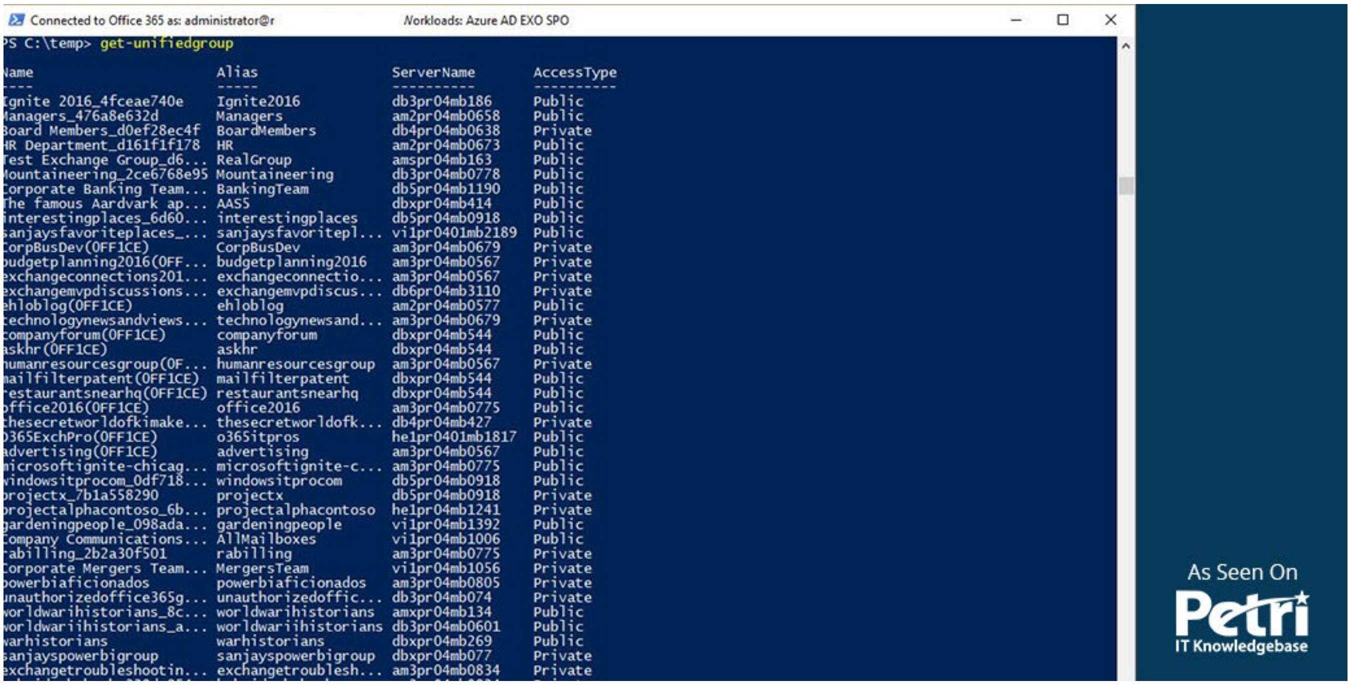
It's possible that Microsoft will give Teams the ability to use classification labels in the future, perhaps after the unification of Office 365 classification labels and Azure Information Protection labels that's promised for later this year. Supporting classification labels might also allow Teams to exploit advanced compliance functionality like disposition review or event-based retention.

A Continuing Journey to Full Compliance

Teams is on a journey to support the full spectrum of compliance features available inside Office 365. This is happening as Microsoft deploys the Teams services into more Office 365 datacenter region (the latest regions added are the U.K. and India), handling increasing customer demand, and rolling out new functionality to support the **transition from Skype for Business Online**. Every week, something changes, so Teams can never be accused of being boring. Which is good, I suppose.

Why PowerShell is a Core Skill for Office 365 Administrators

Published on Petri.com March 29, 2018 by Tony Redmond


Connected to Office 365 as: administrator@r
Norkloads: Azure AD EXO SPO
As Seen On
Petri
IT Knowledgebase

```
PS C:\temp> get-unifiedgroup

Name                      Alias                ServerName      AccessType
----                      -----                ----------      ----------
Ignite 2016_4fceae740e    Ignite2016           db3pr04mb186    Public
Managers_476a8e632d       Managers             am2pr04mb0658   Public
Board Members_d0ef28ec4f  BoardMembers         db4pr04mb0638   Private
HR Department_d161f1f178  HR                   am2pr04mb0673   Public
Test Exchange Group_d6... RealGroup            amspr04mb163    Public
Mountaineering_2ce6768e95 Mountaineering       db3pr04mb0778   Public
Corporate Banking Team... BankingTeam          db5pr04mb1190   Public
The famous Aardvark ap... AAS5                 dbxpr04mb414    Public
interestingplaces_6d60... interestingplaces    db5pr04mb0918   Public
sanjaysfavoriteplaces_... sanjaysfavoritepl... vi1pr0401mb2189 Public
CorpBusDev(OFF1CE)        CorpBusDev           am3pr04mb0679   Private
budgetplanning2016(OFF... budgetplanning2016   am3pr04mb0567   Private
exchangeconnections201... exchangeconnectio... am3pr04mb0567   Private
exchangemvpdiscussions... exchangemvpdiscus... db6pr04mb3110   Private
ehloblog(OFF1CE)          ehloblog             am2pr04mb0577   Public
technologynewsandviews... technologynewsand... am3pr04mb0679   Private
companyforum(OFF1CE)      companyforum         dbxpr04mb544    Public
askhr(OFF1CE)             askhr                dbxpr04mb544    Public
humanresourcesgroup(OF... humanresourcesgroup  am3pr04mb0567   Private
mailfilterpatent(OFF1CE)  mailfilterpatent     dbxpr04mb544    Public
restaurantsnearhq(OFF1CE) restaurantsnearhq    dbxpr04mb544    Public
office2016(OFF1CE)        office2016           am3pr04mb0775   Public
thesecretworldofkimake... thesecretworldofk... db4pr04mb427    Private
O365ExchPro(OFF1CE)       o365itpros           he1pr0401mb1817 Public
advertising(OFF1CE)       advertising          am3pr04mb0567   Public
microsoftignite-chicag... microsoftignite-c... am3pr04mb0775   Public
windowsitprocom_0df718... windowsitprocom      db5pr04mb0918   Public
projectx_7b1a558290       projectx             db5pr04mb0918   Private
projectalphacontoso_6b... projectalphacontoso  he1pr04mb1241   Private
gardeningpeople_098ada... gardeningpeople      vi1pr04mb1392   Public
Company Communications... AllMailboxes         vi1pr04mb1006   Public
rabilling_2b2a30f501      rabilling            am3pr04mb0775   Private
Corporate Mergers Team... MergersTeam          vi1pr04mb1056   Private
powerbiaficionados        powerbiaficionados   am3pr04mb0805   Private
unauthorizedoffice365g... unauthorizedoffic... db3pr04mb074    Private
worldwarihistorians_8c... worldwarihistorians  amxpr04mb134    Public
worldwariihistorians_a... worldwariihistorians db3pr04mb0601   Public
warhistorians             warhistorians        dbxpr04mb269    Public
sanjayspowerbigroup       sanjayspowerbigroup  dbxpr04mb077    Private
exchangetroubleshootin... exchangetroublesh... am3pr04mb0834   Private
```

Office 365 Pros Know PowerShell

Because I come from the Exchange side of the Office 365 house, PowerShell is a natural tool for me to turn to whenever I need to do something with Office 365 that Microsoft hasn't included in the admin tools. The PowerShell coverage for Exchange is deep and extensive, even in the cloud. By comparison, PowerShell is not well covered in other Office 365 applications. Skype for Business Online has some administration functions while **SharePoint Online offers mediocre support**. Planner has no support, and the first version of the **Teams PowerShell module could be so much better**.

Given the spotty coverage in other parts of the service, I guess it should come as no surprise that Office 365 administrators who do not have a background in Exchange might consider PowerShell to be an odd but sometimes useful command-line interface. But that's not the case. Simply put, PowerShell is a core skill for Office 365 administrators.

PowerShell Quirks

It's true that PowerShell has its quirks. Like any scripting language, PowerShell syntax can be baffling and obscure, so using **an IDE is the best approach** for someone starting out. Writing raw PowerShell in the console is for masochists.

PowerShell has significant scalability limitations too, especially inside Office 365 where throttling controls clamp down on anyone who tries to consume resources with abandon. PowerShell will not process tens of thousands of objects rapidly, but that's not its purpose.

If you think you need to process large numbers of Office 365 objects, listen to the **recording of the seminar** by MVPs Alan Byrne and Vasil Michev. The techniques they explain will help you get the job done, but it won't be quick.

Why Admins Need PowerShell

The reasons why Office 365 administrators need to achieve a basic level of competency with PowerShell are varied. Here's my top pick.

The Office 365 Admin Tools are Not Perfect

Beauty is in the eye of the beholder and Microsoft probably thinks that its admin tools are just fine, but some of the more interesting jobs you might want to do need you to plunge into PowerShell. A recent example is the **provision of cmdlets to recover deleted items for users** without the need to log into their accounts.

Another is the **support article** cited in my article on **GDPR data spillage**. The list of steps needed to discover and report all the holds in place for a mailbox that must be temporarily lifted to remove items is long and prone to error. Scripting the retrieval and release of holds for a mailbox would automate the process and make it easier to stand over in court, should the need arise to justify the removal of held information. Finally, I point to the need to **enable mailbox auditing for new mailboxes** to ensure audit data flows into the Office 365 Audit Log. This problem has been around for years and it's surprising that Exchange Online does not enable auditing by default. But you can, with PowerShell.

Microsoft Cannot Anticipate Every Possible Admin Task

Try to write down all the tasks that you think an Office 365 Admin will perform in a year. Once you get past the easy stuff like creating accounts, monitoring usage reports, and so on, it becomes increasingly difficult to anticipate just what admins will be called upon to do. The Office 365 Admin Center and the other associates consoles represent a lot of functionality, but there's always the possibility that you might have to do something that isn't available as a menu choice in a GUI.

Two recent examples are **how to archive inactive Office 365 Groups (and Teams)** and **how to identify when Groups and Teams are not being used**. Microsoft offers the Azure Active Directory expiration policy for Groups, but this is based on time (that is, a group expires after a set period) instead of activity, which creates the possibility that Office 365 could expire and remove your most important teams or groups even though they are in active use daily. You can easily **recover the expired groups** (within 30 days), but that's not the point. It's better to understand what groups and teams are active and act on that basis.

Some Office 365 Features need PowerShell

The group expiration policy has a GUI (in the Azure portal) to work with its settings, but many Office 365 features need admins to run some PowerShell commands to set things up. The Office 365 Groups policy is a good example. If you want to set up **a naming policy** or restrict group creation to a defined set of users, you need PowerShell.

PowerShell Helps You Understand Office 365 Better

Understanding how a technology works is a great way to master it. For instance, running the **Get-MailboxStatistics cmdlet against a group mailbox** reveals its contents. You might or might not be interested in this information, but it is surprising how often detail like this has proven invaluable.

PowerShell Is Not Hard

I am not a programmer now. I used to be, with VAX COBOL and VAX BASIC, in the last millennium, but I can cheerfully hack away with PowerShell and get stuff done. Anyone can too. It's not hard and a ton of useful examples and advice exists on the web (here's **a good start**). Of course, you should never download and run a script in your production environment without carefully examining (and understanding) the code first, but that does not take away from the point that you are not alone.

PowerShell is Fun

Perhaps oddly, PowerShell can be fun too. A sense of achievement comes when a recalcitrant script finally works to make Office 365 give up some secrets or some piece of data becomes more understandable. Although Microsoft might create a perfect nirvana of administration within Office 365, tenant admins need some competence with PowerShell for the foreseeable future. The sooner you start, the better you'll be.

How to Archive Inactive Office 365 Groups (and Teams)

Published on Petri.com February 20, 2018 by Tony Redmond

Office 365 Groups Fade Out Eventually

Sooner or later some of the Office 365 Groups or Teams created within a tenant will become inactive. When this happens, you might be able to remove the group because the data in its resources is no longer needed. However, given the litigious nature of the business world, but some might need to be retained for compliance purposes. There's no out-of-the-box method to mark an Office 365 group or team as inactive, but we can accomplish the goal with PowerShell.

Nice Vision with a Downside

Microsoft's vision for Groups and Teams is that they are collaboration platforms that users should be able to create and use without hindrance. It's a nice idea because it gives users collaboration tools to get things done.

Nice as the vision is, there is a downside. If you allow users to create new groups without oversight, you can end up with groups that are created for a purpose, used, and then discarded. This is not an issue in terms of resources because Microsoft provides the necessary horsepower to create as many mailboxes, sites, and plans as you might need However, it is an issue for address lists as the organization GAL can become very cluttered with groups.

The Joy of Clutter

We've seen similar problems in the past when administrators failed to secure the public folder root. Twenty years after Exchange 4.0 launched public folders on the unsuspecting world, we know all about the problems that free and easy creation cause. Many organizations now struggle to manage public folder rot, let alone the data held in those folders.

I've written about how you can **identify obsolete Office 365 groups with PowerShell**. The basic premise is that a group is inactive and becomes a candidate to be removed when no use is recorded of either the group mailbox, SharePoint site, or (for teams-enabled groups) chats.

Microsoft's **group expiration policy** is another way to address the problem by removing groups once they reach a certain age. Unless, that is, you have a need to keep an obsolete group for compliance purposes.

Keeping Information Until Needed

Let's assume that you spin up a group to assist in the planning and coordination of a financial project. After the project finishes, its group contains conversations about project issues, the calendar of meetings, and all the documents related to the project. This information might have to be retained for an extended period to meet the compliance regime that applies to the company. **Office 365 event-based retention** helps with this problem, but only if you apply suitable classification labels to all the content you need to keep.

One way to keep information for compliance purposes is to put a group into a state where its content is still available but cannot be accessed by users. However, there's no equivalent of **Exchange inactive mailboxes** where holds placed on mailboxes control their retention. A different approach is needed.

Conceptually, the steps to archive a group are straightforward:

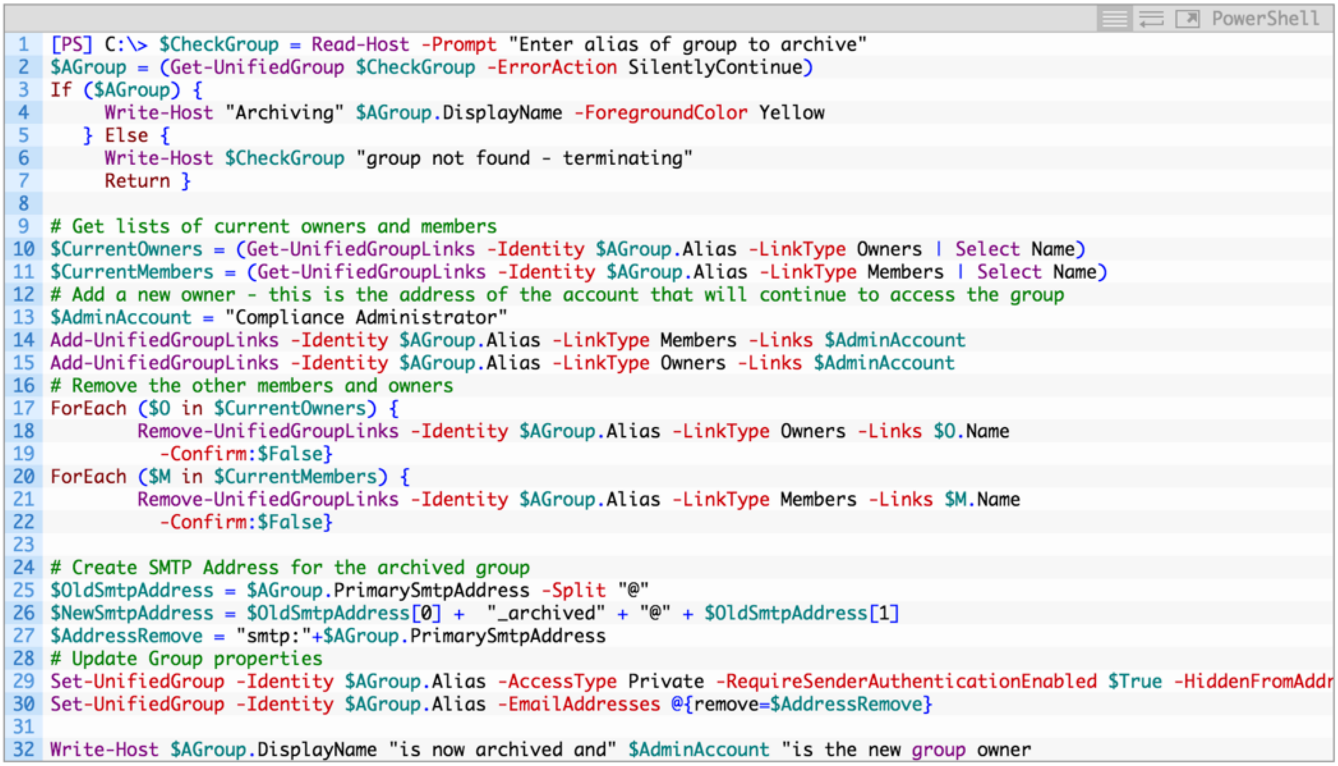
- Add a new group owner. (they must be added as a member first). Ideally, this should be a special compliance administration account instead of a tenant administrator.
- Remove all owners from the group's membership list.
- Remove all users from the group's membership list.
- Ensure that the group is private so that its documents can't be found by Delve r other searches.
- Block email by changing the group primary SMTP address and set *RequireSenderAuthenticationEnabled*property to $True to stop any external email being sent to the group. You could also change the primary SMTP address of the group to stop internal users sending email to the group.
- Hide the group so that it is removed from the GAL.

The archived group is hidden from user view and unavailable through Teams, Planner, or any other group-enabled application.

We can also take advantage of the group custom properties to add some information to mark the group as inactive but retained for compliance. This will make archived groups easier to find if required. The result is that we have a hidden group where the data remains indexed and available for compliance purposes.

PowerShell Solves the Problem

Although Microsoft doesn't provide an out-of-the-box method to archive groups, we can do the job with PowerShell. Here's a script containing the code to do all the necessary work.

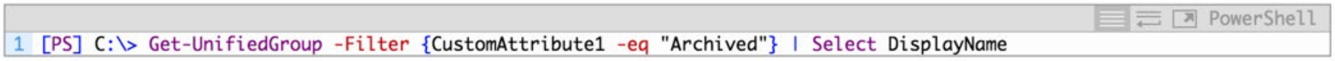


```powershell
[PS] C:\> $CheckGroup = Read-Host -Prompt "Enter alias of group to archive"
$AGroup = (Get-UnifiedGroup $CheckGroup -ErrorAction SilentlyContinue)
If ($AGroup) {
     Write-Host "Archiving" $AGroup.DisplayName -ForegroundColor Yellow
   } Else {
     Write-Host $CheckGroup "group not found - terminating"
     Return }

# Get lists of current owners and members
$CurrentOwners = (Get-UnifiedGroupLinks -Identity $AGroup.Alias -LinkType Owners | Select Name)
$CurrentMembers = (Get-UnifiedGroupLinks -Identity $AGroup.Alias -LinkType Members | Select Name)
# Add a new owner - this is the address of the account that will continue to access the group
$AdminAccount = "Compliance Administrator"
Add-UnifiedGroupLinks -Identity $AGroup.Alias -LinkType Members -Links $AdminAccount
Add-UnifiedGroupLinks -Identity $AGroup.Alias -LinkType Owners -Links $AdminAccount
# Remove the other members and owners
ForEach ($O in $CurrentOwners) {
        Remove-UnifiedGroupLinks -Identity $AGroup.Alias -LinkType Owners -Links $O.Name
          -Confirm:$False}
ForEach ($M in $CurrentMembers) {
        Remove-UnifiedGroupLinks -Identity $AGroup.Alias -LinkType Members -Links $M.Name
          -Confirm:$False}

# Create SMTP Address for the archived group
$OldSmtpAddress = $AGroup.PrimarySmtpAddress -Split "@"
$NewSmtpAddress = $OldSmtpAddress[0] +  "_archived" + "@" + $OldSmtpAddress[1]
$AddressRemove = "smtp:"+$AGroup.PrimarySmtpAddress
# Update Group properties
Set-UnifiedGroup -Identity $AGroup.Alias -AccessType Private -RequireSenderAuthenticationEnabled $True -HiddenFromAddr
Set-UnifiedGroup -Identity $AGroup.Alias -EmailAddresses @{remove=$AddressRemove}

Write-Host $AGroup.DisplayName "is now archived and" $AdminAccount "is the new group owner
```

A short time after the script runs, the group will disappear from clients. The exact time depends on the client. It is fastest for OWA because that client reads from the online directory. It is slowest for Teams because of the need to synchronize the changes with the Teams directory.

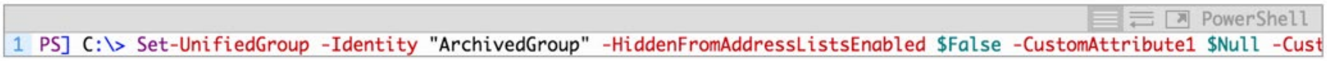
Finding Archived Groups

Marking archived groups through a custom property allows us to identify these groups very quickly. This command lists all groups marked as being archived:



```powershell
[PS] C:\> Get-UnifiedGroup -Filter {CustomAttribute1 -eq "Archived"} | Select DisplayName
```

To restore an archived group to normal status, you need to assign a new owner to the group. The new owner can then add members as required and decide whether the group should be private or public. You would also need to restore the group properties to make it visible in the GAL and to remove the values in the custom properties that mark the group as archived. For example:



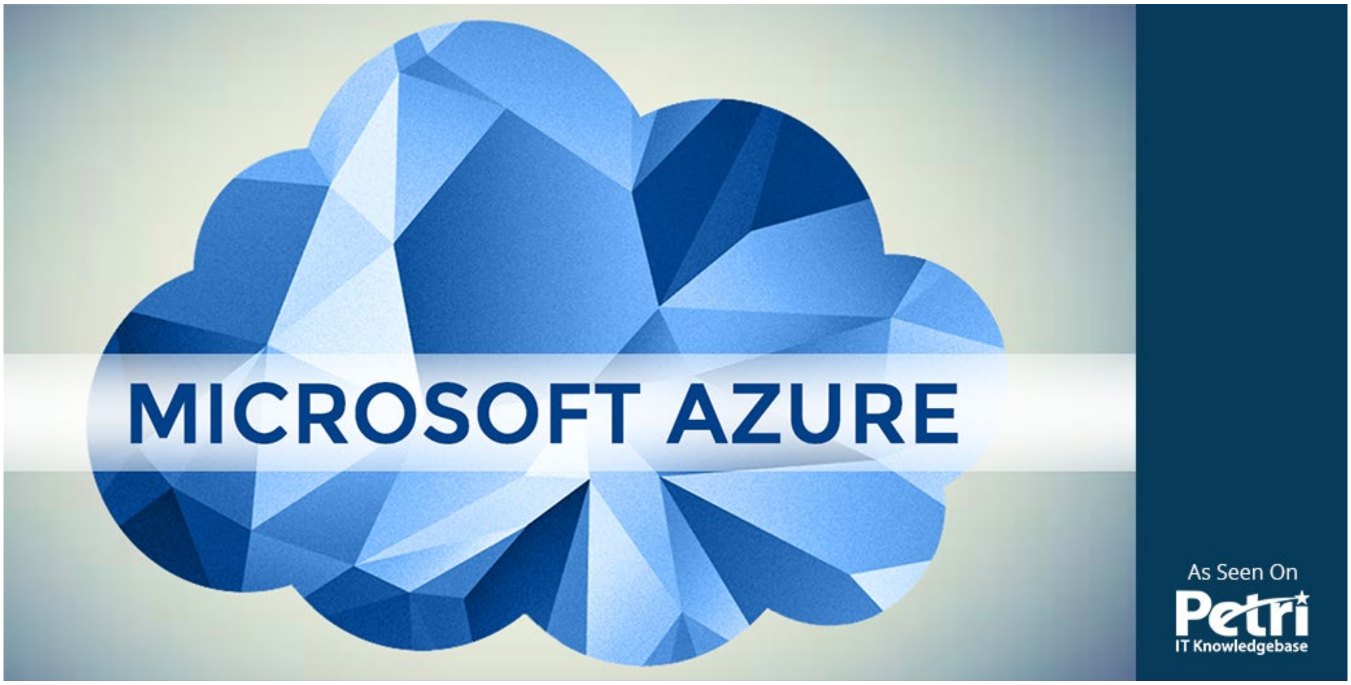
```powershell
PS] C:\> Set-UnifiedGroup -Identity "ArchivedGroup" -HiddenFromAddressListsEnabled $False -CustomAttribute1 $Null -Cust
```

Future Archiving

Hopefully, Microsoft will recognize the need to archive groups and deliver a similar capability in the future (but they will probably **make it a premium feature**). In the interim, the approach taken here is fully supported because none of the steps taken are out-of-the ordinary. After all, it's just PowerShell.

What is Azure SQL Database Managed Instance?

Published on Petri.com April 13, 2018 by Aidan Finn



In this post, I will discuss a new SQL Server option that recently launched a preview in Azure called SQL Managed Instance, enabling you to run a private, managed version of SQL that is almost 100 percent compatible with on-premises SQL Server.

PaaS Versus IaaS

In a **post**, I wrote a few months ago, I compared and contrasted the (then) two options for deploying SQL Server in Azure:

- **IaaS**: You install SQL Server in a virtual machine and live with the cost and pain of managing SQL Server, patching it, upgrading it, backing it up, and so on.
- **PaaS**: You get an Azure SQL database and use it, letting Microsoft keep the code up to date, secure, fault tolerant, manage your backups, and more.

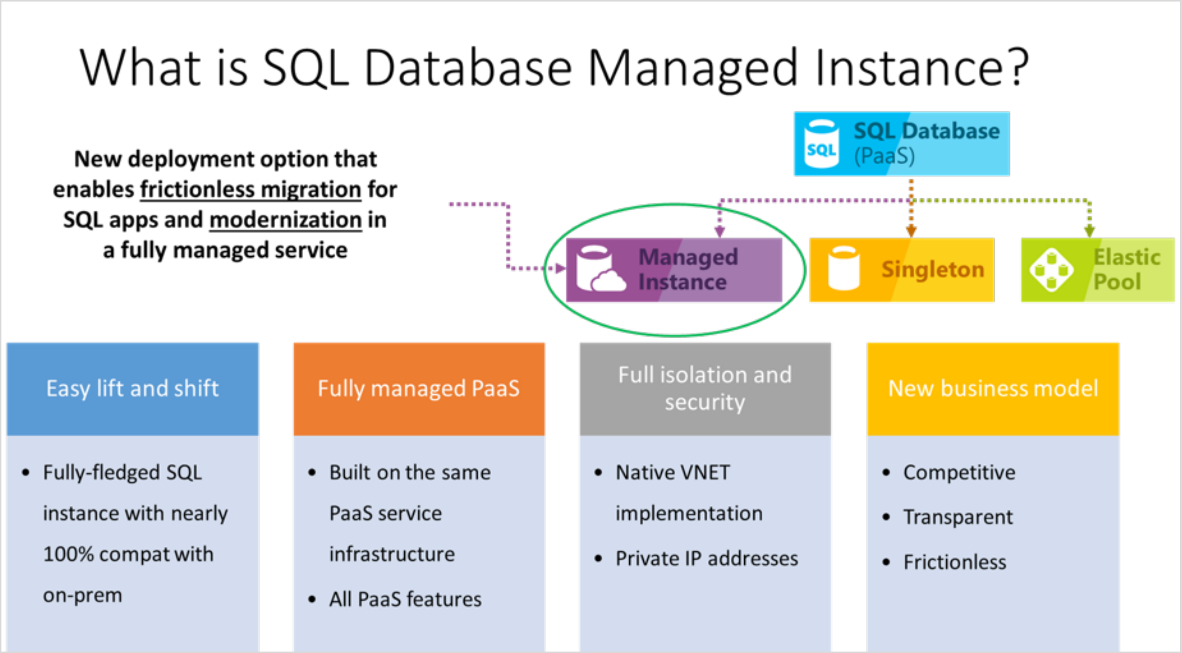
I believe that Azure SQL is a better offering. So why doesn't everyone use it? As one comment on the **post** indicated, sometimes we have old code that expects to find the features of SQL Server and it is simply not there. Azure SQL gives you connection string access to SQL databases but it's not the full-blown lots-of-services SQL Server that you know from the past.

Azure SQL is great for new projects but it's no good for lift-and-shift. It turns out that customers have a lot of lifting-and-shifting that they'd like to do. Those customers have had no choice but to bring SQL Server virtual machines to the cloud, which only extends the old problem. It isn't exactly the most affordable! Microsoft wants more people in the cloud, their cloud to be precise, so they are will to engineer solutions to make it easier.

SQL Managed Instance

Microsoft has provided us with a middle ground. SQL Managed Instance is a solution that will offer near 100 percent compatibility with SQL Server, the same SQL Server that you run on-premises and can deploy with an Azure virtual machine. However, Managed Instances will be a PaaS service where Microsoft gives us the latest version of the code, handles updates, looks after our backups, and all the other things that we expect from a platform.

Note that Microsoft never says 99.9 percent compatibility or 99.99 percent compatibility. They always use the phrase “near 100 percent” compatibility and that’s quite a statement. They’re not there yet with the recently launched Preview of SQL Managed Instance but they plan to be for general availability.



What is SQL Database Managed Instance?

New deployment option that enables frictionless migration for SQL apps and modernization in a fully managed service

SQL Database (PaaS)

Managed Instance

Singleton

Elastic Pool

Easy lift and shift

- Fully-fledged SQL instance with nearly 100% compat with on-prem

Fully managed PaaS

- Built on the same PaaS service infrastructure
- All PaaS features

Full isolation and security

- Native VNET implementation
- Private IP addresses

New business model

- Competitive
- Transparent
- Frictionless

What Is Azure SQL Database Managed Instance? [Image Credit: Microsoft]

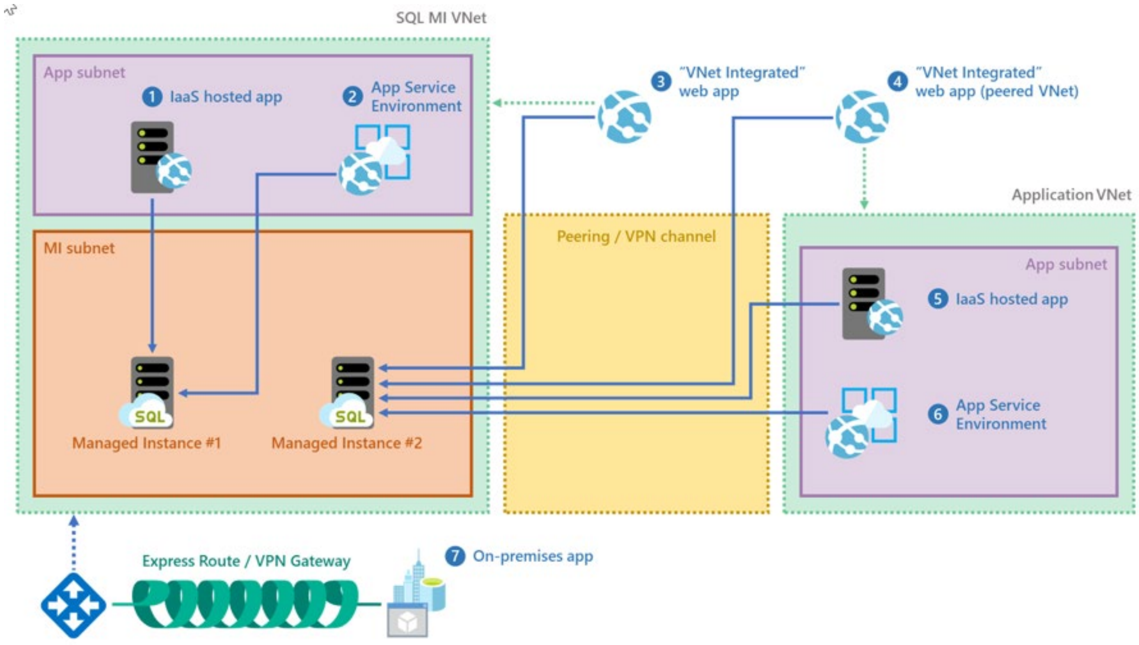
The primary goal of SQL Managed Instance is to give you a path to migrate to Azure. Let’s say that you wish to move an application to Azure and that the database runs on SQL Server. Historically, you had no choice but to move the database machine to Azure too or to redeploy it as another database virtual machine. All that accomplished was that you dropped the tin but most of the operational challenges remained.

Instead, you can use the Azure Data Migration Service to migrate the database to a managed instance running in Azure and immediately take advantage the reduction of operational workload that PaaS can bring to the table. Perhaps, the database will remain there forever, or maybe you will upgrade the application later to take advantage of the lower cost Azure SQL offers.

Note that a managed instance can host up to 100 databases on 8TB of Premium storage with between 5000 and 7500IOPS per data file (database).

Privacy

A secondary reason to consider SQL Managed Instances is that it provides a private connection point to the service via a virtual network.



Azure SQL Database Managed Instance Is Connected to a Virtual Network [Image Credit: Microsoft]

SQL Managed Instance is deployed to a virtual network (ARM only) and can be connected to by other PaaS services and virtual machines across that virtual network. Customers can also have private connections to the database across site-to-site VPN or ExpressRoute connections.

Some customers might choose to deploy SQL Managed Instances because of this privacy, much like how we can deploy App Service Environment (ASE) for the private hosting of app services or web apps.

Some Features

Microsoft highlights a number of features of Azure SQL Database Managed Instances:

- **Data Encryption in Motion**: Transport Layer Security (TLS) is used to encrypt data in motion. Always Encrypted is also used to protect sensitive data in flight, at rest, or during query processing.
- **Dynamic Data Masking**: Have you ever noticed how your credit card is shown to you as a payment option on a shopping site? The last four numbers are shown but everything is masked (X) out? That's the result of Dynamic Data Masking, which also works behind the scenes.
- **Row-Level Security**: You can secure access to sensitive rows based on the characteristics of a user attempting to access the data.
- **Threat Detection**: An automated system that attempts to detect and alert you to suspicious query behavior.
- **Azure AD Integration**: You can use Azure AD for authentication instead of Windows authentication. Note that using Azure AD Connect will bring your Windows (Active Directory Domain Services) accounts

to Azure AD. The Premium version of Azure AD adds multi-factor authentication. You can also use SQL authentication.

Migration

Microsoft mentions two paths for migrating a database to managed instances:

- You can use the Azure Data Migration Service. This managed service provides near-zero downtime and will be best for busy environments or large-scale migrations.
- You can also restore from a backup. First, you would configure on-premises SQL Server to backup to an Azure storage account (blob storage) and then you would restore from that backup. This would be better suited for migrations, where extended downtime would be required (to avoid data loss after the backup).

Pricing

The pricing for managed instances is not nearly as cheap as that of Azure SQL but you are getting a full database instance to yourself! It's probably also more affordable than a mid-large virtual machine. Keep in mind that the instance can host up to 100 databases.

You can deploy Azure SQL Database Managed Instance in a General Purpose tier today and soon there will be a higher cost Business Critical Tier. The general purpose tier is available with:

- **8 cores**: $736.29/month
- **16 cores**: $1,472.58/month
- **32 cores**: $2,208.87/month

The above costs are for US Dollar over 730 hours in the East US region using the RRP pricelist.

If we compare that with a virtual machine alternative, the D8_v3 (8 cores) with SQL Server Standard, not even Enterprise, which is what you get with Azure PaaS, will cost $1,097.92/month.

Also keep in mind that Hybrid Use Benefit, if you have Software assurance on your SQL Server licensing can bring down the managed instance prices by 40 percent – $444.39/month for the 8-core General Purpose option.

A deployment comes with 32GiB of storage. Additional costs will include storage:

- **Capacity**: Each 32GiB block, up to 8TiB, will cost $0.0575/GB
- **IOPS**: Every 1 million requests will cost $0.10. Charging will start after Dec 30th
- **Backup storage**: Will cost $0.05 per GiB. Charging will start after June 30th

Opinion

The managed instance option for Azure SQL could prove to be very popular as a path to cloud transformation for mid-large businesses. I would have liked to have seen a 4-core option for small-mid businesses who also have smaller applications to migrate.

A Checklist for Pricing Azure Virtual Machines

Published on Petri.com April 2, 2018 by Aidan Finn

This post contains a set of things to consider when pricing a virtual machine solution that will eventually run in Microsoft Azure.

Most people struggle to price up solutions when they start working with a utility-based-billing system such as Azure or AWS. The price of a virtual machine isn't just the price of the virtual machine; things such as storage for the disks, backup, disaster recovery replication, and IP addresses are additional costs. All of this isn't necessarily that obvious until you have used Azure and then analyzed the billing report afterward.

This post will show you what to consider when pricing up a virtual machine architecture in Azure, whether you are using Microsoft Excel or one of Microsoft's own pricing tools.

Hours-Per-Month

In Azure, there are 730 hours-per-month. This math is based on multiplying 24 hours by 365 days (8,760) and dividing 8,760 hours- per-year by 12 months (730). Many charges that Microsoft publishes are listed on a per-hour basis, with the per-month charge being estimated, designated by the tilde (~) symbol, based on an average month of 730 hours.

Virtual Machine

The pricing of the virtual machine is a per-minute charge, which is listed as an hourly charge. Start by sizing the machine:

- Series
- Size (processor, RAM, disk speed, data disk numbers, NICs and NIC speed)

Then you will determine how many hours/minutes per-month that the machine will be running.

The next step is to determine the operating system image (Windows, Ubuntu, RedHat, etc) that the machine will be based on. This affects the price. Also affecting the price is if the machine will be pre-installed with SQL Server or BizTalk. Both are charged for on a per-core basis with a minimum of 4 cores.

Note that “S” variants, such as a DS_v3, cost the same to run as a “non-S” variant, such as a D_v3. I always deploy the “S” because the cost is the same. This makes it easy for me to convert from Standard to Premium storage later.

Virtual machine runtime is normally the biggest single charge in this solution (see ExpressRoute later) and it is entirely predictable.

Virtual Hard Disks

You always have to pay for an operating system disk. It is not included in the cost of the virtual machine. If you are using **managed disks**, then this is normally a 128GB disk (P10 or S10). Otherwise, it is normally 127GB. There is a 30GB [smalldisk] option (P4 or S4) in the Marketplace for some Windows images but anyone who intends to own that machine for more than 30 days should steer clear.

All data should go into data disks. This includes Sysvol, databases, and logs on Domain Controllers. Each of these disks is an additional cost.

Virtual hard disk costs are usually the second biggest element in the estimates that I work on and like virtual machines, are under your control and entirely predictable.

Additional Storage

You will likely consume some storage for additional virtual machine management. Table storage from a general purpose v1 (GPv1) storage account is used to store performance metrics (diagnostics data) and blob storage is used to store a small bitmap image of the virtual machine’s console (boot diagnostics). This should probably only be a few cents per month and I normally don’t even account for this or for storage transactions.

Networking

At the very least, you are going to need at least 1 public IP address. Assuming that you are using Resource Manager deployments, this is **a simple flat charge** whether the address is static or dynamic. Note that appliances such as a VPN gateway, load balancer, or a web application gateway will charge for IP addresses.

The basic IP address should suffice in most cases. The Standard IP address is typically only required for zone redundancy.

And that brings us to load balancers. The basic load balancer is free to use. The Standard Load Balancer has a **complicated charging system** based on design and usage.

The next big charge is **outbound data transfer or egress data**. In the case of virtual machines, you are charged for data leaving an Azure region (even between regions). There is no inbound charge. Azure is divided up into zones for this charge and you are billed per GB, with the first 5GB being free.

There is a second kind of internal data transfer charge. If you use VNet peering or you use availability zones, **there is a charge** for data traveling between the virtual networks or between the data centers. Note that global VNet peering has a higher charge.

If you plan to support VPN or ExpressRoute (WAN) connections, then you will require a **VPN gateway**. The Basic size is used in almost every example I have seen, despite the "test/dev" statement from Microsoft, because the spec is sufficient. It is rare that the VpnGw1 size (or higher) is used. This is typically for ExpressRoute or highly-available VPN connections.

And then we get to ExpressRoute. I have never had a customer deploy this WAN connectivity because it has been too expensive. I'll give you the advice I give my customers. Talk to the **WAN vendor first** and if you survive the price shock, then have a look at the **Azure usage pricing** (which isn't bad).

Other virtual appliances, such as the web application firewall/web application gateway are additional costs. Third-party appliances cost the price of the underlying Linux virtual machine plus the cost of the third-party software. Note that bring-your-own-licence (BYOL) might very well end up being cheaper over 1+ years than buying it through the Azure Marketplace.

Backup

Azure Backup has two charges. The first is the **blob storage** (general purpose v1 block blob) that is consumed to store the backups. I normally take the size of the disks of the machines and use that as a basis for estimating the storage consumed. Azure will compress (really effectively) the storage and then keep the differences for each retained recovery point.

The second charge is an **instance charge**, which is based on the total disk size of the virtual machine. Under the covers, the billing system uses the concept of 1 instance, which is a 50-500GB item, and costs $10. Anything that is under 50GB is calculated as half of 1 instances ($5). And anything that is more than 500GB is multiple instances. A virtual machine with 1001GB of disks is 3 (3 * 500) instances ($30).

Disaster Recovery

No cloud replicates your virtual machines to another region automatically. There is a cost to this, so you have to opt-in and pay for the service.

At the very least, there are two charges:

- Double the virtual machine disk storage cost, plus a little extra for processing and up to 24-hour retention of recovery points.
- An Azure Site Recovery charge of $25 per replicated machine.

I did say “to begin with”. Some elements, such as load balancers, application gateways, and so on, will probably need to be pre-deployed, waiting for a disaster. You might need to run virtual machines permanently in the DR site (use a lower spec) because these applications don’t support virtual machine replication (see clustered/replicated databases). This also will require inter-region bandwidth charges for application layer replication traffic and you will run test failovers. Therefore, you will pay for virtual machines running for a few hours every month/quarter/half year/year in the secondary region.

Management Charges

There are charges for managing virtual machines:

- Azure Monitor to monitor and generate alerts/notifications.
- Network Watcher to troubleshoot networking.
- Log Analytics to data warehouse lots of monitoring data.
- Security Center for security monitoring/management. The free SKU is pretty useless in my opinion because most of the recommendations are “buy this thing” noise.

Additional Charges

The above items will get you started but it’s not comprehensive. Are you bringing third-party security or anti-virus software? Are you going to use software for deploying code or running a paid-for CMS? Do you like to use some fancy automation solution? I cannot predict what variations you will add to the mix.

What is App Service Environment?

Published on Petri.com March 2, 2018 by Aidan Finn

In this post, I will explain how you can run Azure App Services in an isolated or virtual network-connected deployment and why, despite the price, it was the right choice for some projects I've been working on.

Normal App Services

When you deploy an app services plan (a set of under-the-cover virtual machines) to host one or more app services in the Free, Shared, Basic, Standard, or Premium Tiers, then the infrastructure that your app services are deployed into are multi-tenant. This means that the virtual machines that make up your app services plan are in a shared pool. Those virtual machines might be dedicated to you, but they come from a shared environment. A set of transparent and hidden front-end servers (offering the load balancing functionality) are shared between all of the tenants (customers) using the virtual machines in this *app services environment*. And finally, because you are in a multi-tenant environment, the app service plan is not connected directly to a virtual network. Although, you can connect your app services to a virtual network via a P2V VPN connection and use this to route externally via a site-to-site VPN connection.

The goal of app services is to make things easy for you. But easy means making some small compromises. For a small number of customers, these compromises are too much. And it is because of this, that Microsoft launched the Isolated tier app services plan, which allows you to deploy your own app services environment (ASE).

App Services Environment (ASE)

The term ASE is normally used to describe a customer's deployment of the isolated tier app services plan, but it's something that I have also heard Microsoft use to describe the hidden pieces of the other tiers. Typically, if you hear ASE, then it's a reference to the Isolated tier.

In short, the Isolated tier app services plan must be deployed into an ASE. The ASE provides a single customer with a completely private deployment of app services. There are a few traits to this:

- **Privacy**: The customer has a completely private, single-tenant deployment, offering them total control over Internet connectivity, security and compliance.
- **Virtual Network**: The virtual machines of the app services plan are connected to a virtual network. This allows for some interesting architectural possibilities, which have caused me to recommend ASE twice in recent weeks. I originally thought that I'd never recommend an Isolated tier because of the cost but I was wrong.
- **Deployment**: There are two deployment types; you can publish an ASE using a public IP address (the same as many other IaaS components in Azure) or using an internal Azure Load Balancer.

IaaS

As several other parts of the Azure PaaS catalogue, ASE is built on IaaS components. One will have to understand virtual networks, IP addresses, load balancers, Network Security Groups, and more. This is more evidence that, even with an advanced PaaS deployment, the future career of IT pros (that are willing to do continuous re-learning) are secure. Although, "disk monkeys" are probably still at great risk.

External ASE

The first type of ASE deployment is an external ASE, using a PIP to make the web apps available to the Internet using a public IP (PIP) address. The first benefit of this approach is that you get a single-tenant (you) ASE but it's still on the Internet. The second benefit of this approach is that the instances of the app service plan(s) that you deploy in the ASE are connected to a virtual network, just like virtual machines. Now some interesting architectural possibilities arise (more on this later).

Internal ASE

The second type of ASE is an internal deployment, where the ASE is shared to the virtual network via an internal Azure load balancer with a private IP address from the virtual network. Note that with this deployment type, you have sole responsibility for managing the DNS of the app services.

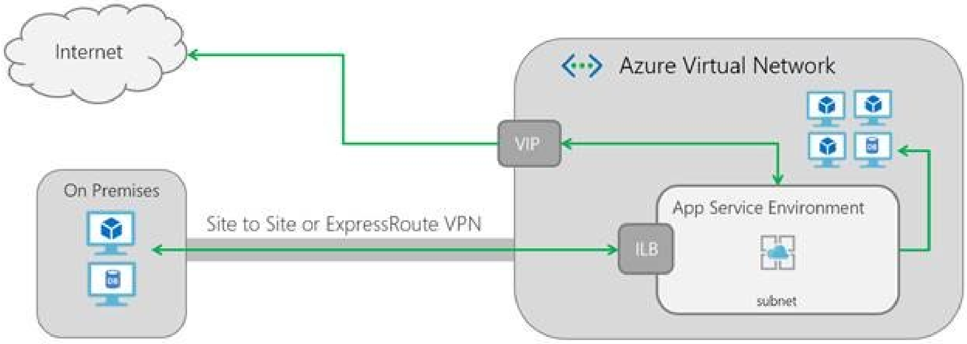
It is up to you if you deploy the app service(s) on the Internet or not, and if you do, how you accomplish it. There are plenty of interesting ways to share a private IP address to the Internet in Azure, including the web application gateway, third-party firewall appliances, and more. The architectural possibilities are interesting!

Virtual Network Connectivity

The reason that ASE has popped up, unexpectedly, in proposals that I have written, is the connectivity to virtual networks. Don't get me wrong, a more traditional app service plan does offer network connectivity:

- **Hybrid Network Connections**: A secure tunnel to a TCP-based service, such as SQL Server, typically running on-premises or in another cloud.
- **VPN**: A point-to-site VPN connection to a virtual network using a gateway, which can route to on-premises via a site-to-site VPN.

The problem with both of those approaches is scale. In one of my proposals, the customer needed many connections to suppliers and partners without deploying any change-making software. If an ASE can be deployed into a virtual network, then a VPN gateway can enable those connections without deploying any software. The higher sizes of gateway support up to 30 site-to-site VPN tunnels.



An Azure Service Environment Connects to a Virtual Network [Image Credit: Microsoft]

The ASE also has the ability to talk directly to virtual machines on the virtual network. That works both ways. Another customer has a preference to use a certain brand of firewall for edge network security. That firewall can be run as a virtual appliance in Azure, so it can be deployed on an edge subnet in the virtual network and route to the private IP address of an internal ASE deployment (internal load balancer).

Or if a customer wishes, the ASE can be published to on-premises users via an ExpressRoute or VPN connection, with no Internet connection at all! The customer gets the cloud benefits of a PaaS deployment but with the security of an isolated installation.

Summary

When I saw the fixed cost of an ASE (~$1,043.82/month RRP in East US) plus the cost of the isolate tier instances (starting at ~$219/month RRP in East US), I thought I would never deploy ASE. However, when we compared the architectural, technical, and operational (developer) benefits with the alternatives, ASE with the Isolated app services tier was a no-brainer.

How Can I Store Secrets in Azure?

Published on Petri.com February 22, 2018 by Aidan Finn

In this post, I will tell you about a service in Azure called Key Vault, which you can think of as secret storage/handling-as-a-service.

Secrecy

It's probably fair to say that a concern that most prospective and current cloud customers have is secrecy. Some things must not be known outside of an organization. Sometimes secrets must not be known by more than a few people. Some secrets must be kept in the cloud:

- A developer wants to store private encryption keys for use by an application.
- A service provider doesn't want to know or handle the secrets of its customers.
- An Azure virtual machine will have BitLocker enabled and the key must be stored in the cloud.
- An operator wants to store some passwords for later reference.

Microsoft introduced Azure Key Vault to handle these kinds of secrets. When it launched, it seemed like a service that I would have little to do with. But more and more, Microsoft is finding more ways to use Key Vault, making the service one of the things that are hard to avoid in Azure.

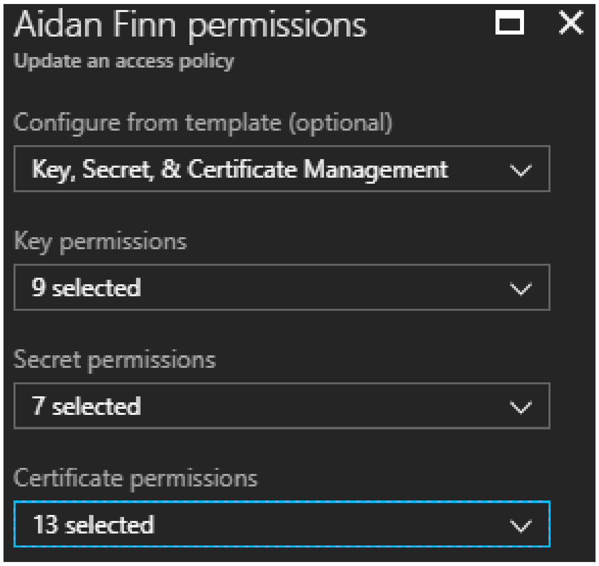
Reliable Storage

Any secrets that you generate or store in Key Vault are kept in the same physical data centers as the applications that have stored and are using the secrets. That provides you with performance. But much like with many systems in Azure, the vaults are replicated within the region and also to the documented **paired region**. This is a twinned region, at least 150 miles away, and normally in a similar regulatory zone such as in the EU or in the USA. In the event of a region failover (I haven't witnessed one yet), it can take a few minutes for the key vault to come online in the paired region and the secrets will be in read-only mode. A fail-back can occur and then the vault returns to read and write mode.

Securing Your Secrets

In the USA, Federal Information Processing Standards (FIPS) is considered an important measuring stick for security. Microsoft has two levels of certification based on how you store a secret in Key Vault. The support levels available depend on the tier (price/features) of key vault that you deploy.

A Standard tier key vault only supports software keys. These are processed inside of cryptographic modules with FIPS 140-2 Level 1 validation or higher. A Premium tier key vault also offers hardware keys. In this case, a hardware security module (HSM) validated to FIPS 140-2 Level 2 or higher will handle the secrets for you.


Aidan Finn permissions
Update an access policy

Configure from template (optional): Key, Secret, & Certificate Management

Key permissions: 9 selected

Secret permissions: 7 selected

Certificate permissions: 13 selected

Figure 1: Azure Key Vault Permissions [Image Credit: Aidan Finn]

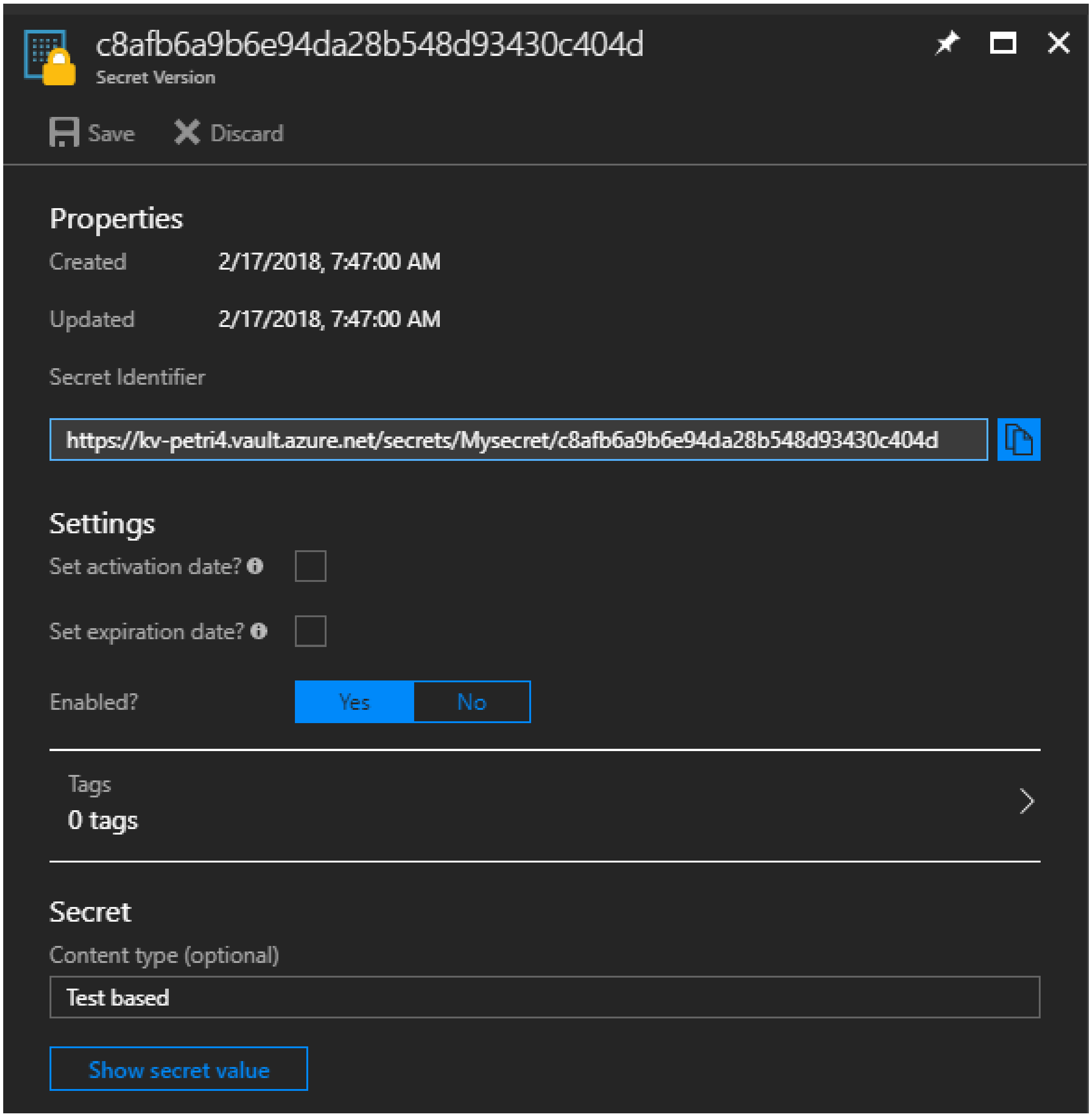
A key vault has its own permission system for the contents, independent of what is done at the resource or resource group level. When you create a key vault, you will define a default administrator, who has a set of key permissions, secret permissions, and certificate permissions. This means that only a subset of Azure administrators/developers/operators can manage or even see the secrets that are stored in the vault.

Abstraction

Let’s say that you wish to build an online application that requires a set of encryption keys for handling data transfers securely. Typically, those secrets are stored with the application, leaving them vulnerable to theft and misuse by a hacker. If you use Key Vault, the keys are stored in key vault, not with the application. The application is provided with a URI to access the keys and use them, effectively allowing the developer to treat the code as being somewhat untrusted. This is the same sort of approach that the same developers use for credit card payments, using an API to offload payments to a more trusted handler.

Getting Started

After I started to look at Key Vault, I realized that I should have been using this service for years and I have to start telling my customers about it. For example, without doing any PaaS or development, I can store secrets (text) very easily in a key vault and make them available to me at any time:



c8afb6a9b6e94da28b548d93430c404d
Secret Version

Properties

Created 2/17/2018, 7:47:00 AM

Updated 2/17/2018, 7:47:00 AM

Secret Identifier

https://kv-petri4.vault.azure.net/secrets/Mysecret/c8afb6a9b6e94da28b548d93430c404d

Settings

Set activation date? □

Set expiration date? □

Enabled? [✓ Yes] No

Tags
0 tags

Secret

Content type (optional)

Test based

Storing Text-Based Secrets Securely in Azure Key Vault [Image Credit: Aidan Finn]

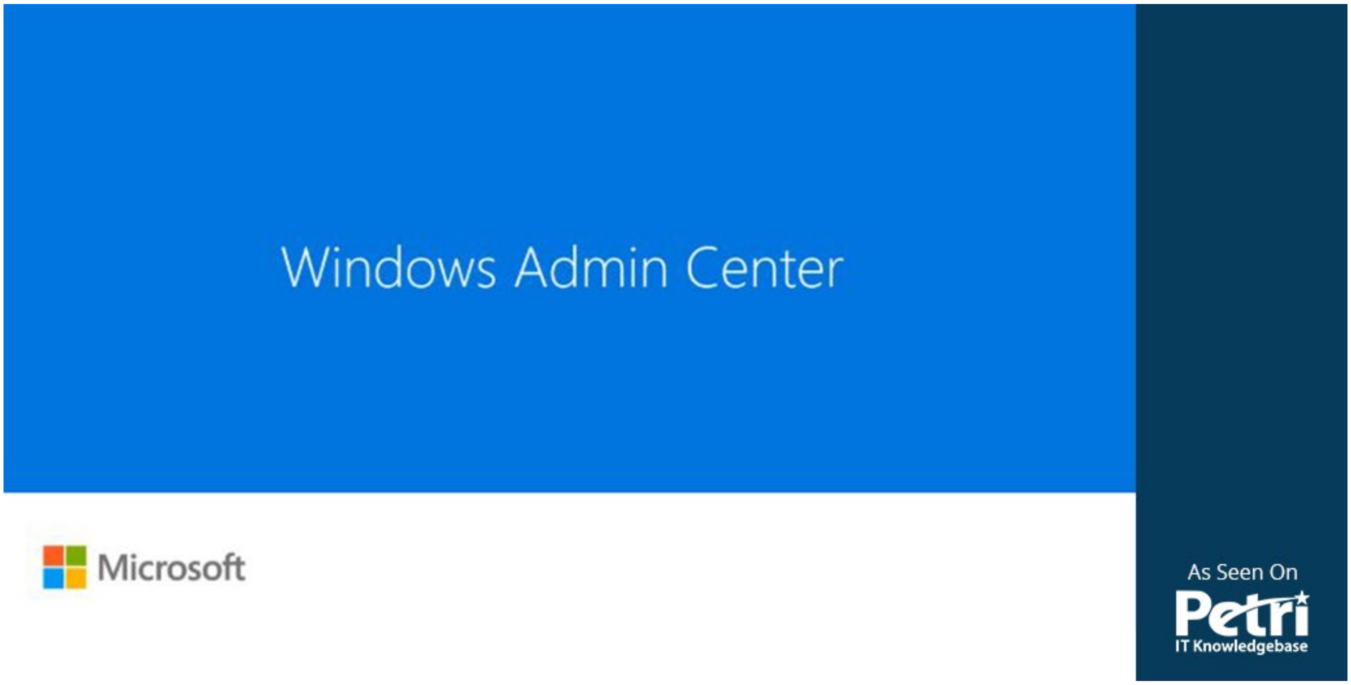
Examples might be:

- Passwords
- Passphrases for on-premises deployments of Azure Backup

These are simple secrets that are easily created in the Azure Portal and will improve how most admins are keeping these secrets today (a spreadsheet or Word document).

Getting Started with the Windows Admin Center

Published on Petri.com April 19, 2018 by Russell Smith



In this *Ask the Admin*, I'll provide a general overview of the Windows Admin Center, which was released earlier this month.

The GUI management tools in Windows Server haven't changed much over the years. There have been a few new ones, like Server Manager and the Active Directory Administrative Center, but by and large, no revolutionary changes. If you are familiar with Computer Management, Device Manager, or Active Directory Users and Computers (ADUC), you will know what a typical Microsoft Management Console (MMC) looks like. It's a hierarchical tree that can be expanded to view configuration options. MMCs have an unfriendly UI and use Remote Procedure Calls (RPC) to manage remote computers, meaning that they are not firewall-friendly.

The Windows Admin Center (WAC) is a complete reimagination of not only the UI but also the back end. WAC is a website for managing either the local or remote servers via a gateway that uses PowerShell Remoting and Windows Management Instrumentation (WMI) over WinRM. The gateway can be installed on Windows Server 2016, Windows Server version 1709, Windows Server 2019, and Windows 10. WAC can manage Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012. It can also manage Hyper-V Server, Azure VMs, Azure Backup, highly-converged infrastructures (HCI), and more.

Because the gateway is a webserver application, administrators can connect to it from the public Internet and the local area network. Connecting to a gateway, rather than directly to the nodes you want to manage, allows for more flexibility and the option to easily secure communications.

Install a Gateway in Windows Server

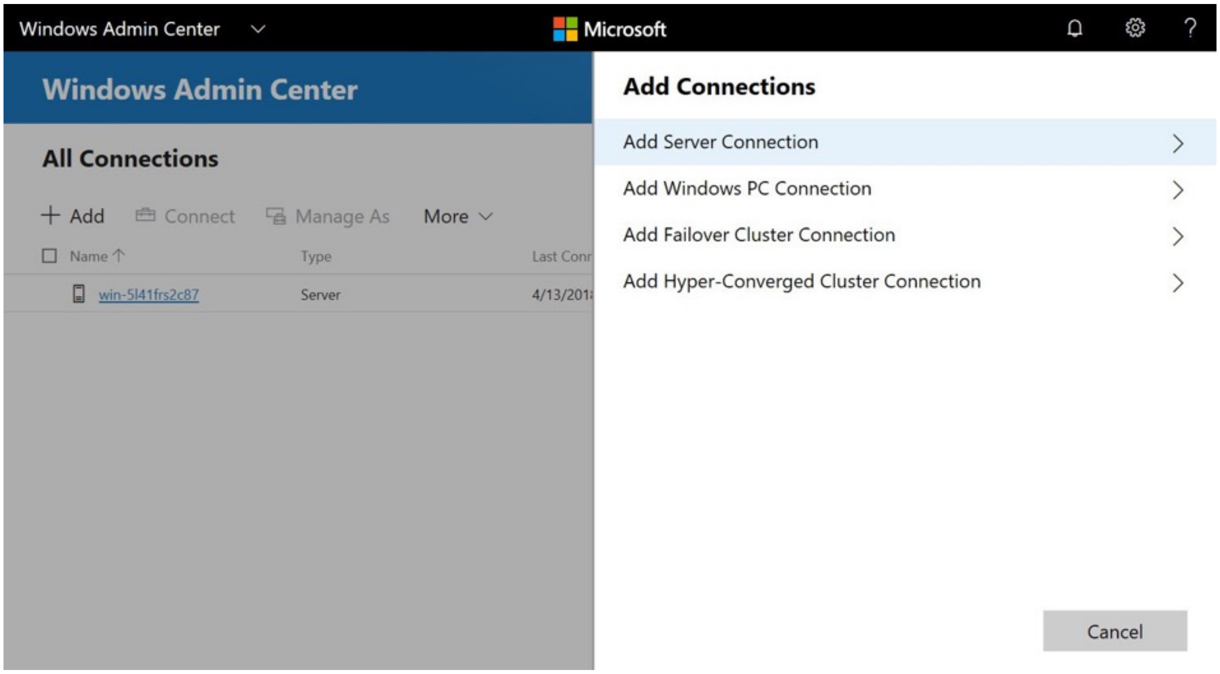
The gateway can be installed on Windows 10, for small-scale environments, or on a server. If you want to manage Windows Server 2012 or Windows Server 2012 R2, you'll need to install the Windows Management Framework (WMF) version 5.1 on devices running those operating systems. I installed the gateway in Windows Server 2019. You can download WAC **here** from Microsoft's website. If you want to install WAC on Windows Server Core, read **How to Install the Windows Admin Center in Server Core** on *Petri*.

Once you've installed the gateway, open the WAC website using the link provided on the desktop. To connect to WAC from a remote device, type the name of the server on which the WAC gateway is installed in the browser address bar. If you changed the default port (443), add a colon followed by the port number specified when WAC was installed to the end of the URL. WAC supports Microsoft Edge and Google Chrome.

Unless you provided a certificate during the WAC gateway install process that is trusted by the devices from which you will connect to the gateway, you'll need to bypass the security warnings in your browser when connecting to WAC. In a production environment, you should not let the installer generate a certificate but instead provide your own. Once connected, you'll need to provide a username and password to connect to the gateway. This should be an account on the gateway device.

Using Windows Admin Center

The *All Connections* screen shows you the list of servers you can manage. The gateway server appears by default. You can add servers, failover clusters, and hyper-converged clusters by clicking **+ Add**. All you need to do is type the DNS name of a remote server or import a list of servers from a .txt file.



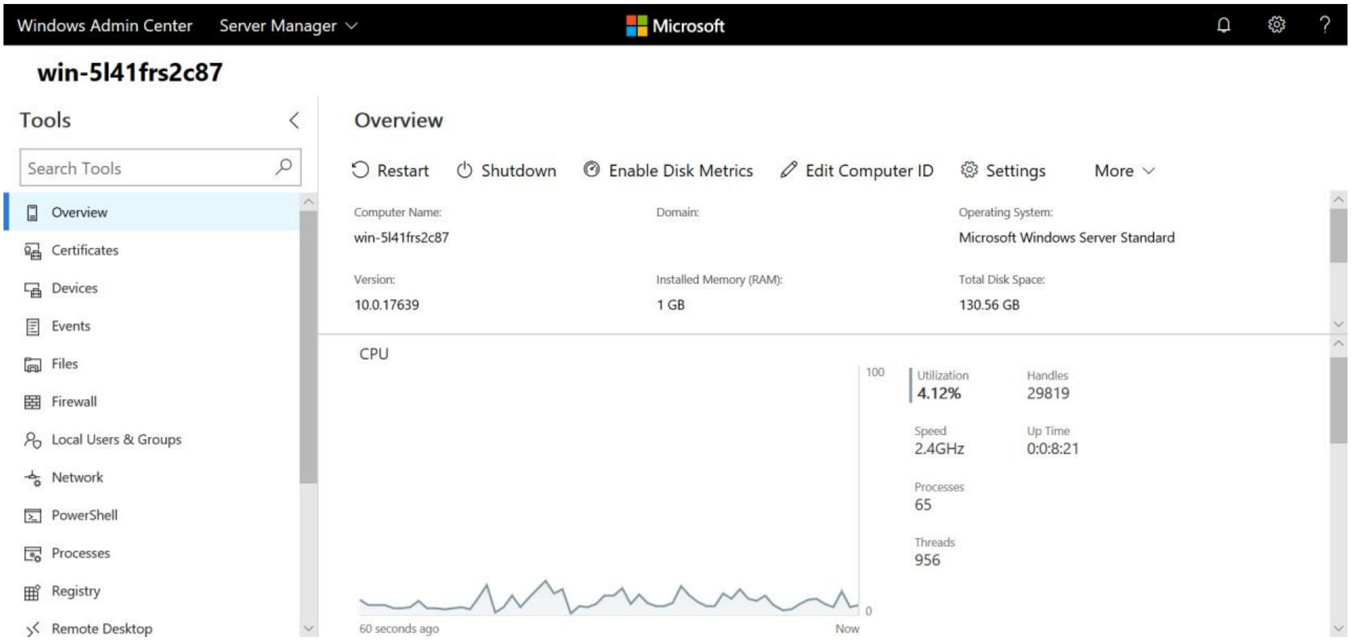
Connecting to Remote Servers Using the Windows Admin Center (Image Credit: Russell Smith)

You can authorize remote servers and clusters using the Windows account you are logged in to your PC with, credentials you provide manually for the session, or Local Administration Password Solution (LAPS) credentials. For more information on LAPS, see [Secure Local Administrator Accounts with the Local Administrator Password Solution (LAPS) Tool]() on *Petri*.

Connect to a Server

Click on a server on the *All Connections* screen. You'll need to enter a username and password to make a connection to the server. An overview of the server's health is displayed by default, similar to that displayed by Task Manager. The graphs for CPU, memory, disk, and network are updated in real time and you can restart and shutdown the server. The *Settings* option allows you to edit *system* and *user* environment variables, enable or disable Remote Desktop, and manage WAC Role-Based Access Control (RBAC). Currently, there are three access roles:

- **Windows Admin Center Administrators** – Allows users to view and manage most tools.
- **Windows Admin Center Hyper-V-Administrators** – Allows users to manage Hyper-V virtual machines and switches. Other tools are available in read-only mode.
- **Windows Admin Center Readers** – Allows users to view most tools but doesn't allow them to make any changes.



Computer Name: win-5l41frs2c87

Domain:

Operating System: Microsoft Windows Server Standard

Version: 10.0.17639

Installed Memory (RAM): 1 GB

Total Disk Space: 130.56 GB

Utilization 4.12%

Handles 29819

Speed 2.4GHz

Up Time 0:0:8:21

Processes 65

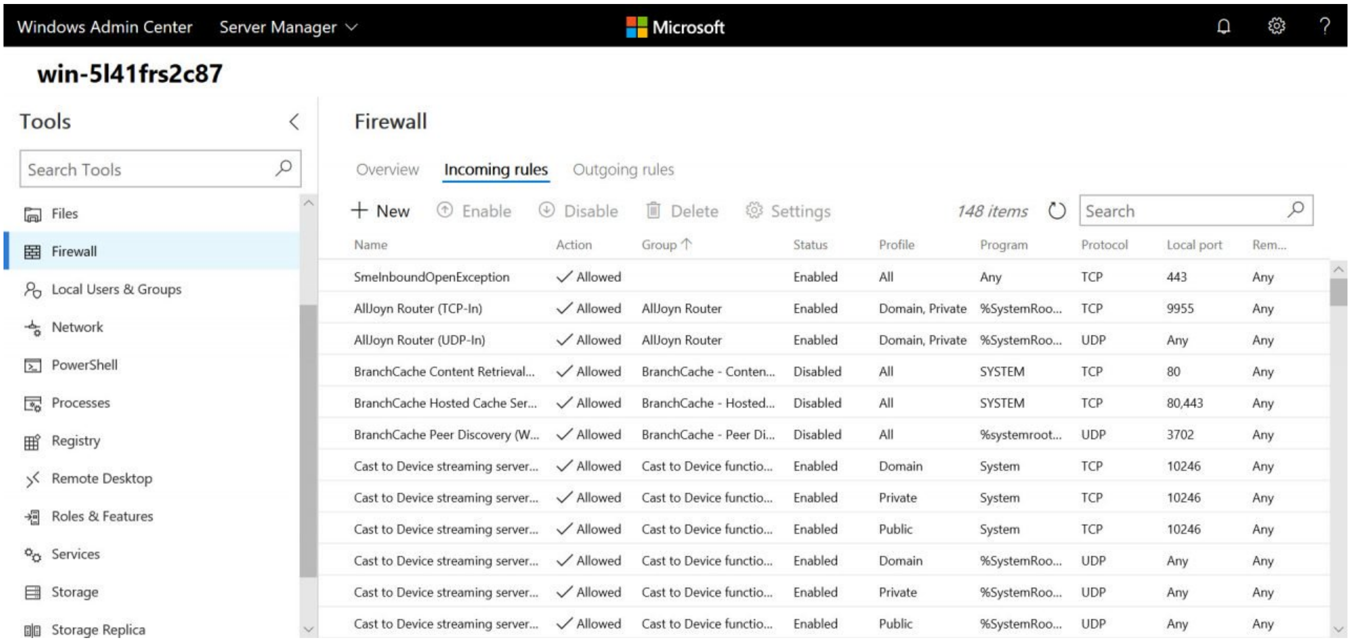
Threads 956

Server Overview in the Windows Admin Center (Image Credit: Russell Smith)

There's a list of tools on the left, which you can search. Most things you'd expect are present, including the ability to manage services, the registry, devices, files, Windows Update, virtual machines if the Hyper-V role is installed, events, Windows Firewall, network adapters, and local users and groups.

The tools allow you to carry out basic tasks. For example, *Services* lists the services installed on the server and their status. You can start and stop services, and set the service startup type. WAC has improved since the initial beta release (Project Honolulu) and now it is possible to set service recovery options and specify a service account.

Device Manager lets you disable devices but there's no access to more advanced configuration, although you can update drivers. Events can be exported and filtered but advanced options found in Event Viewer are missing, like Custom Views. But it is possible to search events and apply a filter to narrow down the results. Other tools, like Firewall, Local Users and Computers, and Roles and Features are quite well padded out and will allow you to perform most common administrative tasks without resorting to other tools.



Name	Action	Group ↑	Status	Profile	Program	Protocol	Local port	Rem...
SmeInboundOpenException	✓ Allowed		Enabled	All	Any	TCP	443	Any
AllJoyn Router (TCP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Private	%SystemRoo...	TCP	9955	Any
AllJoyn Router (UDP-In)	✓ Allowed	AllJoyn Router	Enabled	Domain, Private	%SystemRoo...	UDP	Any	Any
BranchCache Content Retrieval...	✓ Allowed	BranchCache - Conten...	Disabled	All	SYSTEM	TCP	80	Any
BranchCache Hosted Cache Ser...	✓ Allowed	BranchCache - Hosted...	Disabled	All	SYSTEM	TCP	80,443	Any
BranchCache Peer Discovery (W...	✓ Allowed	BranchCache - Peer Di...	Disabled	All	%systemroot...	UDP	3702	Any
Cast to Device streaming server...	✓ Allowed	Cast to Device functio...	Enabled	Domain	System	TCP	10246	Any
Cast to Device streaming server...	✓ Allowed	Cast to Device functio...	Enabled	Private	System	TCP	10246	Any
Cast to Device streaming server...	✓ Allowed	Cast to Device functio...	Enabled	Public	System	TCP	10246	Any
Cast to Device streaming server...	✓ Allowed	Cast to Device functio...	Enabled	Domain	%SystemRoo...	UDP	Any	Any
Cast to Device streaming server...	✓ Allowed	Cast to Device functio...	Enabled	Private	%SystemRoo...	UDP	Any	Any
Cast to Device streaming server...	✓ Allowed	Cast to Device functio...	Enabled	Public	%SystemRoo...	UDP	Any	Any

Managing Windows Firewall Rules in the Windows Admin Center (Image Credit: Russell Smith)

Unlike the original Project Honolulu release, WAC includes a tool that makes a remote connection to the server using PowerShell. This will come in handy considering that WAC is still missing some tools, like scheduled tasks, DHCP, DNS, and IIS.

The Future of Windows Server GUI

Microsoft has been pushing Server Core for several years now, even going as far as forcing organizations to choose the full GUI or Server Core at install time. Previously, it had been possible to move between the two after installing Windows Server. The Windows Admin Center isn't supposed to replace all the Remote Server Administration Tools (RSAT) that most system administrators will be familiar with but it does cover a lot of the basics. WAC is extensible. Out of the gate, it includes Azure AD integration for gateway authentication and the ability to manage Azure virtual machines and Azure Site Recovery.