



The premium event for IT-professionals

Feb. 1-3rd in Oslo Spektrum



The Azure Security Dojo Live

Andy Malone MVP

CEO: Quality Training (Scotland) Ltd

Andrew.malone@quality-training.co.uk

Follow me on Twitter @AndyMalone

Andy Malone

(United Kingdom)

Microsoft MVP (Enterprise Security)
Microsoft Certified Trainer (20 years)
Founder: Cybercrime Security Forum
Worldwide Event Speaker
Author: The Seventh Day
www.AndyMalone.org





Lesson 1 The Trust Vs Knowledge Theory

Common Cloud Misconceptions

- My current computer systems will work just as well in the cloud as they do today
- It is easy to change from one cloud provider to another whenever I want to
- One vendor is more secure than another
- Vendors Cannot Access User Data
- Being in the Cloud Ensures my Privacy!
- Most users are brand loyal and will always stick to one vendor
- All Data is encrypted

Common Cloud Frustrations

- At Mercy of Vendors Security Policy
- Easy to Migrate Data in, but Difficult to Migrate out
- Users unsure on how to encrypt / Decrypt data
- How can users Backup Encryption Keys
- Vendors often Vague about Where Data is Stored.
- 85% Vendors Based in USA



A close-up photograph of a woman's face. She has dark skin, curly brown hair, and is wearing dark eyeshadow and red lipstick. Her eyes are closed, and she is holding her right hand up to her forehead, with her fingers resting near her temple. This gesture typically signifies stress, headache, or frustration. The lighting is dramatic, with strong highlights on her forehead and nose.

Common Cloud Frustrations

- Difficulty to decipher the encryption terms cloud vendors use to describe their security
- Doing so would require discrimination between
 - Transport encryption
 - Data encryption
 - Metadata encryption
- Encryption at rest vs. in motion & then most importantly Evaluating key management & access

I don't
trust words,
I TRUST
ACTIONS.

What do these Vendors Have in Common?





SPIDEROAK

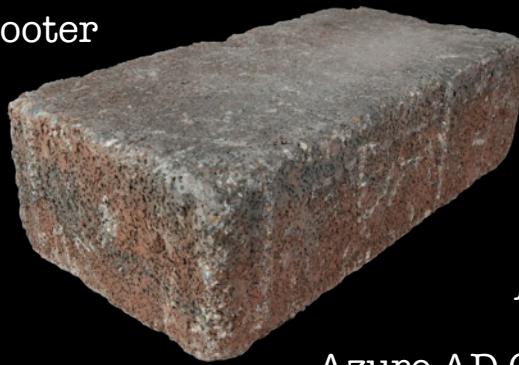
Zero Knowledge Systems

"We don't know the names of your files, the names of your folders, the date they were created or last modified or accessed, their size, their checksums or hashes...in short we know nothing about your data except how much you store."



Lesson 2 Azure & the Brick Wall Theory

Azure Security = The Brick Wall Theory



Azure Security Portal

Azure Information Protection

BitLocker Disk Encryption

Azure Security Troubleshooter

Azure Security Documentation

Container Security

Multi Factor Authentication

Azure Forensics

Azure Security Health Monitoring

Azure AD Privileged Identity Management

Azure AD Connect Health

Hybrid Management

Microsoft Anti Malware For Cloud Services & Virtual Machines

Azure Key Vault

Azure AD Identity Protection

Azure Business Continuity



**Traditional Security is
not working**

Data in Transit at Risk!



How is Microsoft Addressing the Problem?



Azure Identity
Solutions



Secure
Deployment



Azure Security
Management



Troubleshooting
& Monitoring



legal &
Compliance





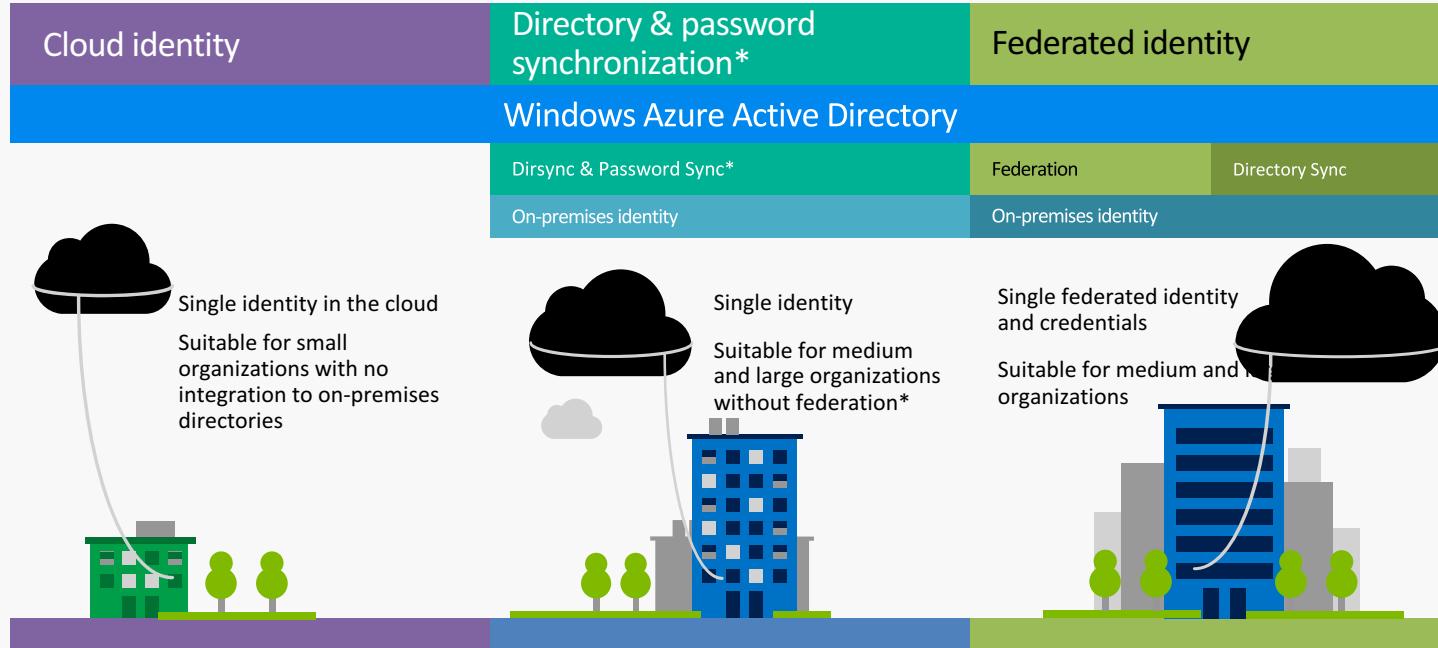
Lesson 3 Identity is the New Control Plane

Identity has its Challenges ...

- Managing and controlling identity and user access
- Encrypting communications and operation processes
- Securing networks
- Managing threats
- Governance & Compliance
- Law Enforcement



Identity is the new Control Plane ...

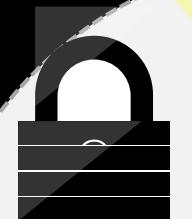
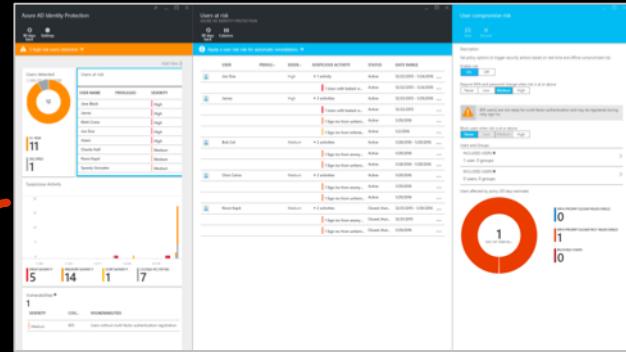


Azure Identity Protection

- Risk based Conditional Access automatically protects against suspicious logins and compromised credentials
- Detect and remediate configuration vulnerabilities to improve your security posture
- Gain insights from a consolidated view of machine learning based threat detection



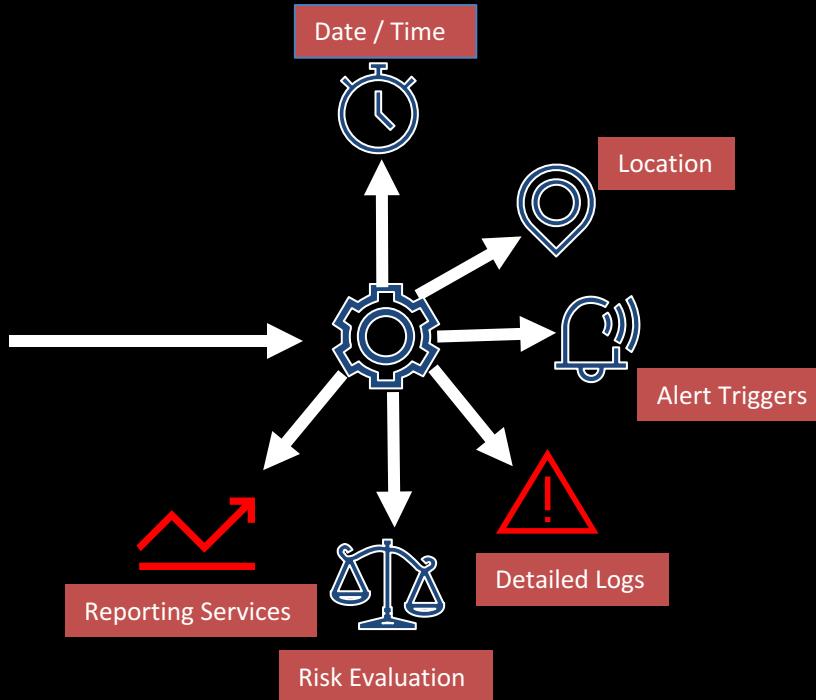
MFA Challenge
Risky Logins
Change bad credentials
Block attacks



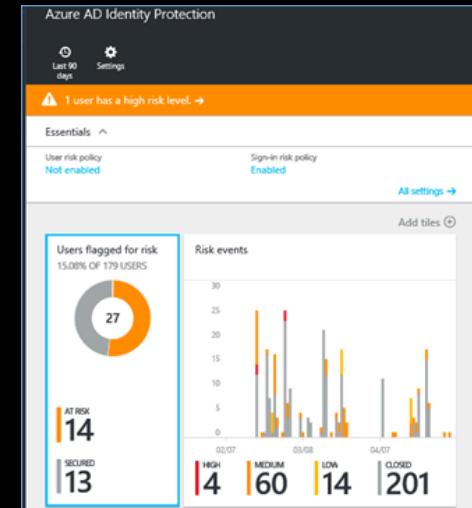
Azure AD Identity Protection



User Logs in



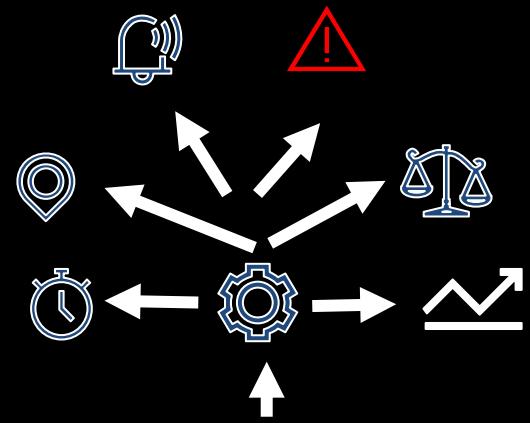
Azure Identity Protection



Detailed Heuristics

Azure AD Identity Protection!

- Provides Detailed Reports on:
- Users with leaked credentials
- Irregular sign-in activity
- Sign-ins from possibly infected devices & unfamiliar locations
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from impossible travel
- & Much More ...
- * Requires Azure AD Premium 2





Demo: Azure AD Identity Protection



Lesson 4 Plug The Admin Holes

Beyond Role Based Admin Control?



Chandler Bing
Chandler.bing@Trainmeon365.onmicrosoft.com
Analyst, Sales

Edit user roles

Choose the admin role that you want to assign to this user. [Learn more about administrator roles](#)

User (no administrator access)

Global administrator

Customized administrator

Alternative email address

Save **Cancel**



Chandler Bing
Chandler.bing@Trainmeon365.onmicrosoft.com
Analyst, Sales

Edit user roles

Choose the admin role that you want to assign to this user. [Learn more about administrator roles](#)

User (no administrator access)

Global administrator

Customized administrator

Billing administrator

Exchange administrator

Password administrator

Skype for Business administrator

Service administrator

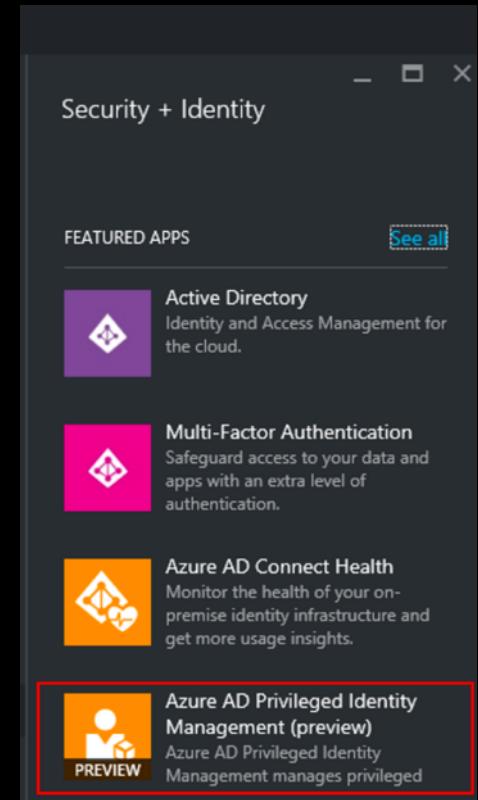
SharePoint administrator

Save **Cancel**

Azure AD Privileged Identity Management

Azure AD Privileged Identity Management helps you

- See which users are Azure AD administrators
- Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune
- Get reports about administrator access history and changes in administrator assignments
- Get alerts about access to a privileged role



Azure AD Privileged Identity Management

- Alerts that point out opportunities to improve security
- The number of users who are assigned to each privileged role
- The number of eligible and permanent admins
- Ongoing access reviews

The screenshot shows the Azure AD Privileged Identity Management interface. At the top, there are three buttons: Settings, Refresh, and Wizard. Below this is a header bar with the title "Privileged Identity Management" and the organization name "Contoso".

The main area is divided into several sections:

- Activity:** Displays two alerts:
 - 2 ! Roles are being activated too frequently
 - Administrators aren't using their privileged roles
- Users in admin roles:** Shows 17 users.
- Audit history:** A button to view audit logs.
- Quick start:** A button to get started.
- Role summary:** A table showing the count of users assigned to various roles.

ROLE NAME	MFA ENABLED	USERS	ACTIVE	ELIGIBLE
Security Reader	Yes	1	1 (100%)	0 (0%)
Global Administrator	Yes	9	5 (56%)	4 (44%)
Privileged Role Administra...	Yes	11	3 (27%)	8 (73%)
Security Administrator	Yes	9	3 (33%)	7 (78%)
Password Administrator	Yes	2	0 (0%)	2 (100%)
User Administrator	Yes	2	1 (50%)	2 (100%)
- Access reviews:** A section for managing access reviews.

Azure AD Privileged Identity Management

Global Administrator

The screenshot shows a user interface for managing privileged identities. At the top, there are buttons for Add, Filter, Refresh, Group, Review, and Settings. Below is a search bar with a magnifying glass icon. The main area has three columns: USER, PERMISSION, and EXPIRATION. The data is organized under a section titled "GLOBAL ADMINISTRATOR".

USER	PERMISSION	EXPIRATION
Jennifer Davey jenniferdavey@contoso.com	Permanent	-
Lee Sperry leesperry@contoso.com	Eligible	-
Jack Smith jacksmith@contoso.com	Eligible	-
Admin admin@contoso.com	Permanent	-

Security Administrator

Role activation details

Activate Deactivate

NAME
Lee Sperry

EMAIL
leesperry@contoso.com

ACTIVATION
Eligible

EXPIRATION
-

Request role activation

Security Administrator

* Reason for role activation ⓘ

* Ticket number ⓘ

Ticketing system

This screenshot shows a "Request role activation" form. It includes fields for the reason and ticket number, and a dropdown for the ticketing system. The "Activation" status is currently set to "Eligible".



Demo: Azure Privileged Identity Management

Azure AD Privileged Identity Management

The screenshot displays the Azure AD Privileged Identity Management interface. On the left, a list of permanent administrators is shown, each with a blue user icon, name, email, activation status (Permanent), is active status (Yes), and expiration date (never). On the right, a detailed view of a selected temporary administrator, Jennifer Davey, is displayed. The interface includes buttons for managing the user's status (Make active, Make temp, Make perm, Remove) and a search bar at the top.

NAME	ACTIVATION	IS ACTIVE?	EXPIRATION
John Doe O365Admin@Natantion...	Permanent	Yes	never
Admin admin@Natantionmicro...	Permanent	Yes	never
Marcel Ferro Marcel@Natantionmicrosoft...	Permanent	Yes	never
Scotty Lock scottyllock@Natantionm...	Permanent	Yes	never
Lee Spary LeeSpary@Natantionml...	Permanent	Yes	never
Jack Smith NatanOutlook@Natant...	Permanent	Yes	never

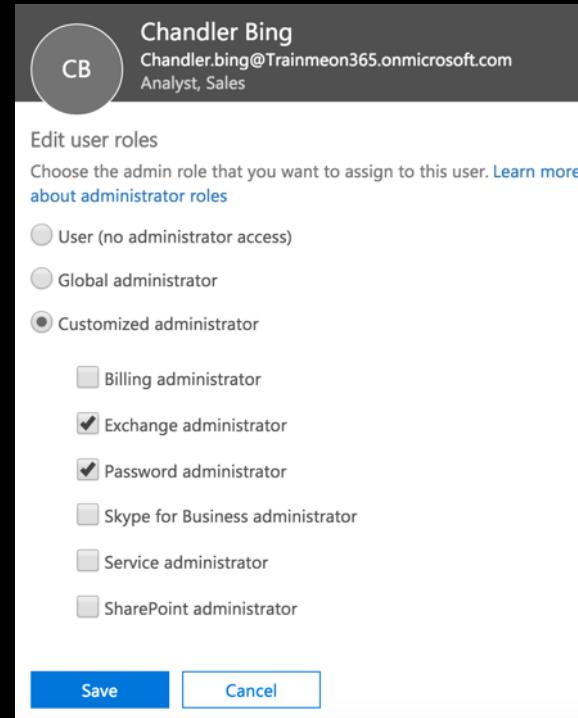
TEMPORARY

Jennifer Davey Jennifer.davey@Natantion...	Temporary	-	-
---	-----------	---	---

Manage both Permanent & Temporary Admins (JIT)

Top Tip: JIT & JEA AD Privileged Admins

- Global Admins can update which users are permanently assigned to roles in Azure AD.
- PowerShell cmdlets like `Add-MsolRoleMember` and `Remove-MsolRoleMember`
- The Azure classic portal as described in assigning administrator roles in Azure Active Directory
- Cannot be done in the Office 365 Portal yet!
- Global Admins can make temporary role assignments by making users eligible for a role
- An eligible admin can activate the role when they need it, and then their permissions expire once they're done.



Top Tip: Here's Lookin' at you Kid!

Start recording user and admin activities

X

When you turn this on, user and admin activity in your organization will be recorded to the Office 365 audit log and available to view in a report.

Turn on

Cancel

★ Recommended for you ...

Search for activity



Want to know what your users and admins are doing? Start recording activities in Office 365.

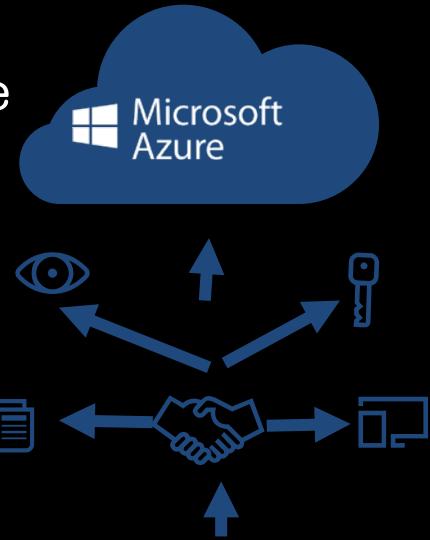
Start recording now



Lesson 5 Azure Multi-Factor Authentication

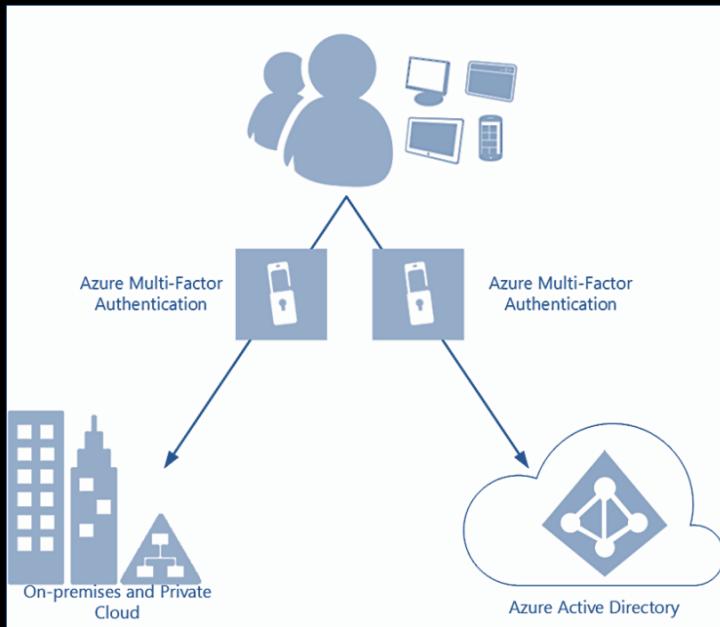
Azure Multi Factor Authentication!

- Method of authentication requiring more than one verification method
- Combines device as something you have or Somewhere you are
- Password Something you know
- Fully supports Biometrics (Something you are)
- Adds a critical second layer of security to user sign-ins and transactions
- Available for Azure, Office 365 & Hybrid Deployments



Azure Multi Factor Authentication!

- Authentication Methods:
- Phone call
- Text message
- Mobile app notification
- Users can choose the method they prefer
- Mobile app verification code
- 3rd party OAUTH tokens



Azure Multi Factor Authentication!

multi-factor authentication

users services

Note: only users listed here will be affected.
Before you begin, make sure you have a mobile device or computer with a camera available.

bulk update

View: Sign-in methods

DISPLAY NAME

Andrew M...@bing.com

Chandler B...@Trainmeon365.onmicrosoft.com

HQSales@Trainmeon365.onmicrosoft.com

Jean Luc Picard@Trainmeon365.onmicrosoft.com

Joey Tribiani Joey.trbionani@Trainmeon365.onmicrosoft.com Disabled

John Snow SnowS@Trainmeon365.onmicrosoft.com Disabled

Monica Geller monica.geller@Trainmeon365.onmicrosoft.com Disabled

Ross Geller ross.geller@Trainmeon365.onmicrosoft.com Disabled

! About non-browser applications

After multi-factor auth is enforced, users will need to create app passwords to use non-browser applications such as Outlook or Lync.

For security reasons app passwords are not available to admins, who will be able to sign in only with the browser.

enforce multi-factor auth cancel

quick steps

Disable

Enforce

Manage user settings

User	Email	Status
Joey Tribiani	Joey.trbionani@Trainmeon365.onmicrosoft.com	Disabled
John Snow	SnowS@Trainmeon365.onmicrosoft.com	Disabled
Monica Geller	monica.geller@Trainmeon365.onmicrosoft.com	Disabled
Ross Geller	ross.geller@Trainmeon365.onmicrosoft.com	Disabled

Azure Multi Factor Authentication!

multi-factor authentication

users service settings

app passwords

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app

remember multi-factor authentication

- Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60):

Save

Multi Factor Auth PowerShell Step by Step

1: install the Microsoft Online Services Sign-In Assistant

Next Install the Azure Active Directory Module for Windows PowerShell

Get-ExecutionPolicy (If the output is anything other than "unrestricted", run the following command)

Set-ExecutionPolicy Unrestricted -Scope CurrentUser

Multi Factor Auth PowerShell Step by Step

2: Connect to MsolService via PowerShell

```
$UserCredential = Get-Credential  
Import-Module MSOnline  
Connect-MsolService -Credential $UserCredential  
$auth = New-Object -TypeName  
Microsoft.Online.Administration.StrongAuthenticatio  
nRequirement  
$auth.RelyingParty = "*"
```

3: Choose the MFA State \$auth.State = "Enabled"

Multi Factor Auth PowerShell Step by Step

4: Choose the date - Any devices issued for a user before this date would require MFA setup

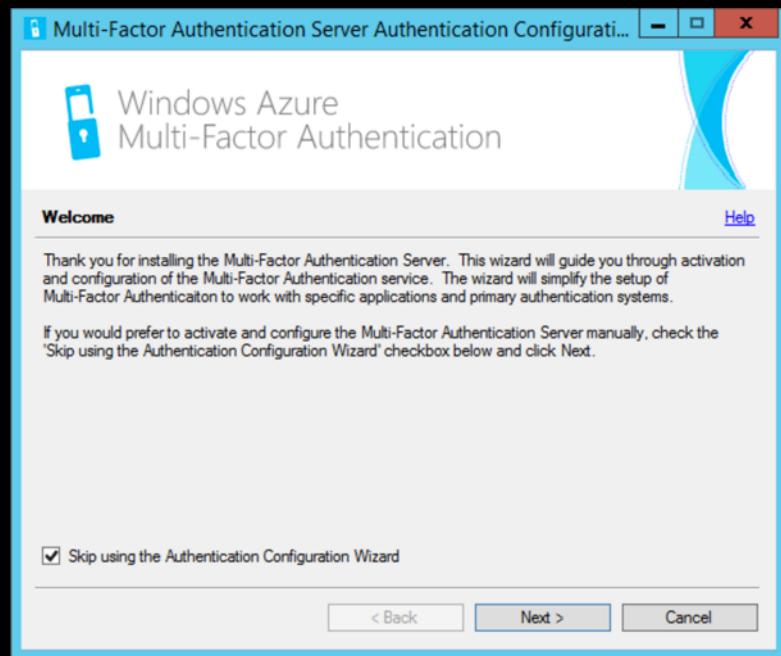
```
$auth.RememberDevicesNotIssuedBefore = (Get-Date)
```

5: Enable MFA for all users: Get-MsolUser -All | Foreach{ Set-MsolUser -UserPrincipalName \$_.UserPrincipalName -StrongAuthenticationRequirements \$auth }

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>

Top Tip: Combine Multi Factor Auth with SSO

- On the Local ADFS Federation Server install WindowsAzureSDK-x64.exe
- On the Local ADFS Federation Server run the PowerShell Cmdlet run Register-ADFSAuthenticationProvider
- Run the Microsoft Azure Multi Factor Authentication Wizard - Server Authentication Wizard
- You're all set!



Import from Active Directory

[Help](#)

Domain: contoso.com

List Search

View: Container Hierarchy

Username	Name	Email Address	Mobile
AAD_808273a96d74			
Administrator@contos...		Administrator@contos...	
bsimon@contoso.com	Simon, Britta		
MSOL_808273a96d74			

Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Microsoft Exchange Security Groups
Microsoft Exchange System Objects
Program Data
System
Users

User filter:

Display users 4

Import: Selected Users Display limit: 1000

Settings Method Defaults Language Defaults

Add new users
 Update existing users
 Disable/Remove users no longer a member

Import phone:

Backup:

Enabled

Send email

Assign new PIN to updated users

Email

Settings Email Content

Phone Call

- Standard
 - New User
 - User Enrollment
 - Updated User
- PIN
 - New User
 - User Enrollment
 - Updated User

Text Message

- One-Way
 - OTP
 - New User
 - User Enrollment
 - Updated User
 - OTP + PIN
 - New User
 - User Enrollment
 - Updated User
- Two-Way
 - OTP
 - New User
 - User Enrollment
 - Updated User
 - OTP + PIN
 - New User
 - User Enrollment
 - Updated User

Mobile App

- Standard
 - New User
 - User Enrollment

Format: Plain Text
From: NOT SPECIFIED
Cc:
Subject: Welcome to Multi-Factor Authentication
Attachment:

Your account has been configured to use Multi-Factor Authentication. Multi-factor authentication involves something you know (your username and password) and something you have (your phone). When you sign on, you will continue to use the same username and password. Before your sign on is complete, you will receive a phone call asking you to enter your PIN followed by the pound (#) key to confirm your sign on. If you don't confirm the sign on by entering your PIN and pressing #, the sign on will be denied.

Your account has been configured as follows:

Phone: <phone\$>
PIN: <\$pin\$>

Please reply to this email if this phone number is not correct or you would prefer a different phone number.

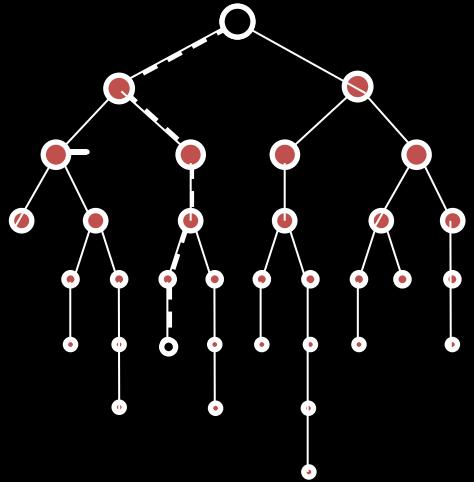
Note: You should only enter your PIN when you receive the Multi-Factor Authentication call if you are actually signing on. Otherwise, someone may be trying to sign on with your username and password and you should report this potential fraud to your IT administrator.

Edit... **Resend...**



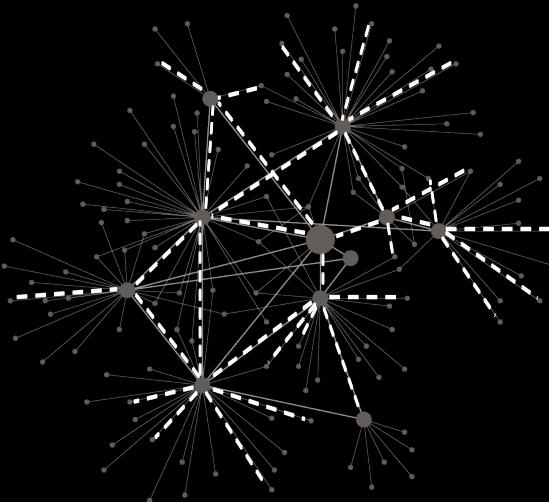
Lesson 6 Protecting your Info Azure Style!

The Changing Structure of Data!



TRADITIONAL HIERARCHIES

INFORMATION MOVES SLOWLY
COMMAND AND CONTROL

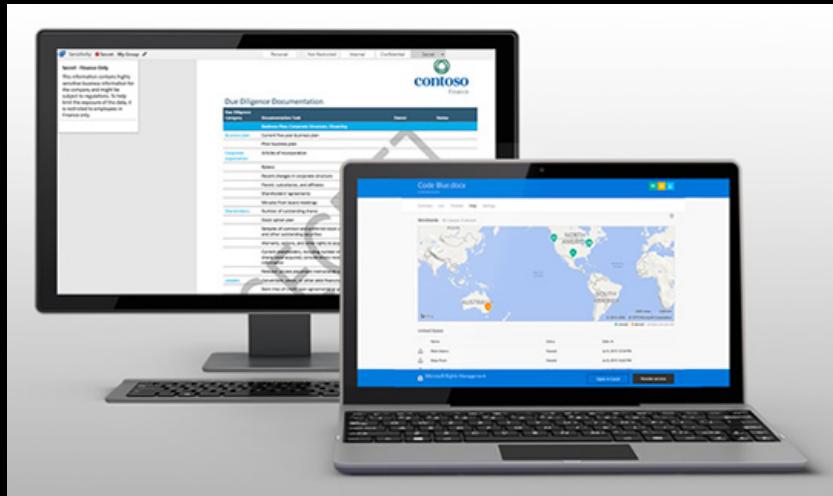


RESPONSIVE NETWORKS

INFORMATION TRAVELS FAST
LEARN AND ADAPT

Azure Information Protection: Wild West Hero

- Permissions Bleed
- Once data is outside organization, its beyond the realm of your control
- Anyone can plagiarise
- Content easily copied
- Potential Copyright Infringement Issues
- Plausible Deniability Reins
- Lack of Compliance



Azure Information Protection



Document
Classification &
Labelling



File Encryption



Rights
Management

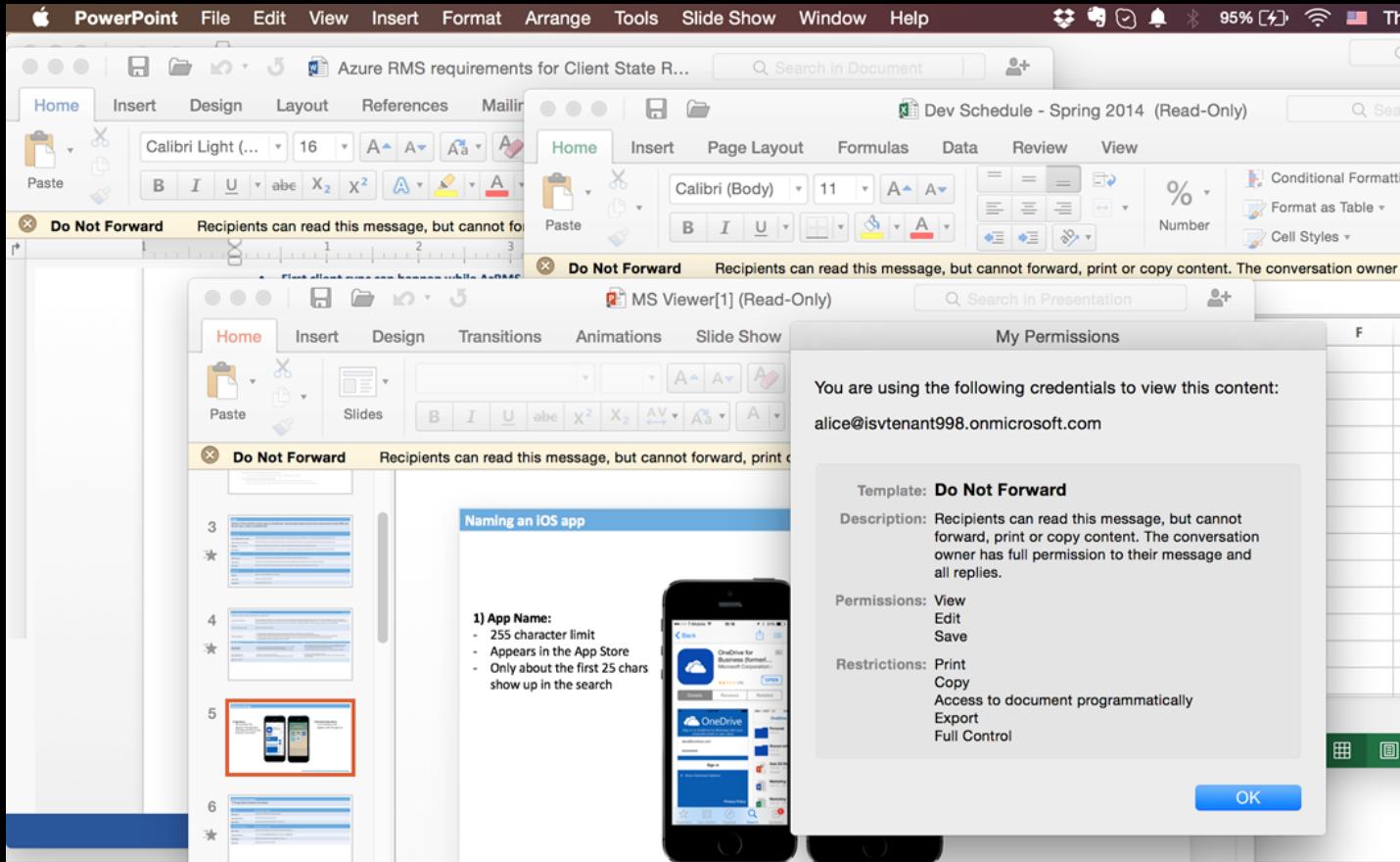


Detailed Auditing,
Tracking &
Reporting

Simple
Configuration



Azure AD Rights Management Services





Demo: Azure Information Protection

Azure Information Protection Office 2016 Add in

The screenshot shows the Microsoft Azure portal interface on the left and a Microsoft Word document window on the right.

Azure Information Protection Settings:

- Sensitivity:** Personal
- Configure a title and tooltip for the Information Protection client on user devices:**
 - Title:** Sensitivity
 - Tooltip:** Information Sensitivity consists of six distinct levels (Personal, Public, Internal, Confidential, Secret, and Office). Identify the risk of exposing the information to unauthorized users inside or outside the business. Mark documents and emails with labels to share them with others. Otherwise select an appropriate label to reflect the sensitivity of the content.
- Configure the name, tooltip, and additional settings of each label; Order the labels according their sensitivity level:**

LABEL NAME	TOOLTIP	MARKING
Personal	For personal use only. This data will not be monitored.	
Public	This information is internal and can be used by everyone.	
Internal	This information includes a wide spectrum of internal data.	✓
Confidential	This data includes sensitive business information. Ex...	✓
Secret	This data includes highly sensitive information for th...	✓
Office 365 Book Source	A document marked as a source file for the Office 3...	

- Default Label:** Personal
- Justification Note:** Users must provide justification when lowering the sensitivity level (for example, from Confidential to Public).

Word Document Content:

Master-Microsoft-Office-365-like-a-pro.-Office-365-for-IT-Pros, 3rd-Edition-is-essential-reading-if-you-want-to-maximize-your-use-of-Microsoft's-Office-365-cloud-services.¶

Companies-are-migrating-to-Office-365-at-increasing-speed.-Over-70-million-active-users-and-1.2-million-tenants-already-use-Office-365-.Exchange-Online-is-called-"the-gateway-drug-to-the-cloud"-by-Microsoft-CEO-Satya-Nadella-because-it-is-usually-the-first-workload-to-move-from-on-premises-servers-into-the-cloud.-But-as-you'll-learn-in-Office-365-for-IT-Pros,-once-you've-moved-mail-across,-there-are-plenty-of-new-and-exciting-advantages-to-be-gained-from-the-wide-breadth-of-functionality-that-exists-elsewhere-inside-Office-365.¶

Previously-published-as-"Office-365-for-Exchange-Professionals",-Office-365-for-IT-Pros, 3rd-Edition-adds-more-than-250-pages-of-new-content-covering-essential-business-productivity-features-such-as-Office-365-Groups,-Office-365-Planner,-Dive-Analytics,-SharePoint-Online,-and-OneDrive-for-Business-in-addition-to-all-of-the-information-you'd-ever-want-to-know-about-Exchange-Online.¶

This-is-the-only-Office-365-book-available-today-that-is-constantly-refreshed-and-updated-with-new-information.-You-will-receive-regular-updates-that-keep-pace-with-developments-in-Office-365,-which-means-that-Office-365-for-IT-Pros-remains-a-valuable-reference-for-you-long-after-you-first-read-it.¶

Original-published-on-June-1,-2016,-Office-365-for-IT-Pros, 3rd-Edition-was-last-updated-on-July-13,-2016.¶

Written-by-three-highly-experienced-Microsoft-Most-Valuable-Professionals-(MVPs),-Office-365-for-IT-Pros-is-a-practical,-hands-on-reference,-based-on-experience-gained-by-working-in-real-life-projects-with-a-range-of-customers-since-the-introduction-of-Office-365-in-June-2011.¶

Throughout-its-400,000-words,-Office-365-for-IT-Pros-includes-in-depth-instructions-(including-over-700-PowerShell-code-samples)-for-provisioning,-migrating,-and-administering-the-many-different-services-and-features-that-exist-within-the-Office-365-cloud.¶



Lesson 7 Conditional Access

Conditional access

Conditions



User attributes

- User identity
- Group memberships

Devices

- Is Domain Joined
- Is Compliant
- Platform type
- Lost or Stolen

Application

- Per application policy
- Mobile apps or Cloud apps

Other

- Location (IP Range)
- Risk Profile

Requirements



Allow
Block
MFA
Enroll

Microsoft Azure
Office 365



On-Premises applications



Demo: Azure Conditional Access



Lesson 8 Lessons in Compliance!

Microsoft Data Centres Policies & Procedures Ensure Compliance

- Highly Secured Physical Environments
- Multiple Redundancy Model
- Small number of Staff
- Separation of Duties & Roles
- Strict Security Policies & Procedures
(Failure=Dismissal)
- Managed Data Destruction Policies
- PII & Non PII Stored Separately
- Free & Paid services Stored Separately
- Customer Breach Notification Policy
- Law enforcement Breach Notification Policy



Example: Office 365 Compliance Centre

- Single portal Solution
- Set up Alerts
- View Audit Logs
- Set Security Policies
- Import / Export / Archive Data
- Search & Investigate
- eDiscovery
- Service Assurance

The screenshot shows the Microsoft Security & Compliance Center interface. On the left is a dark blue sidebar menu with the following items:

- Home
- Permissions
- Security policies
- Data management
- Search & investigation
- Reports
- Service assurance

The main content area is titled "Home" and features a "Join the evolution" banner. Below it is a "Search for activity" section showing a user icon and a "Who's been sharing files?" link. To the right is a "Your one-stop shop" section with a "Secure by design" card (showing a padlock icon), a "Data management" card (showing binary code and a storage icon), and a "Search & investigate" card (showing a magnifying glass over a cloud icon). Each card has a "Read more..." link.



Demo: Office 365 Compliance Centre



Lesson 8 Elementary my Dear Watson ...

Digital Forensics

“Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data.”

But the World has Changed

- Need to update Security Policies & Procedures
- Develop & Maintain an Incident Response Plan
- Understand how will this effect your Disaster Recovery
- Need to Develop a Hybrid Backup Solution
- Ensure that any move to the cloud ticks all your organizations, countries & industries legal & compliance boxes



Surely Forensics Just became 50% Harder?

- Perceived Loss of data control
- No access to physical infrastructure
- Legal issues of multi-jurisdiction
- Multi-tenancy and multi-ownership
- Lack of tools for larger-scale distributed and virtualized systems
- No standard interfaces
- Little provider cooperation
- Difficulties in producing forensically sound and admissible evidence in court



Actually it's now 50% Easier

- Improvement in Forensic Tools
- Users often Require Verified Accounts
- Improved Logs & Auditing Procedures
- Better eDiscovery & In Place Hold
- Shrink Wrapped Crime Scene (VMs)
- (CSA) Cloud Security Alliance – Strive to be Compliant
- Growth in Cross Platform Identity Standards –
SAML 2.0 – Oauth 2.0
 - Microsoft Account – Google – Amazon – Facebook - LinkedIn
- Easier to Migrate in and Out of Cloud
- Improvement in International Legal Co-operation



It's not just where but How Data is Stored?

14+

Copy Count

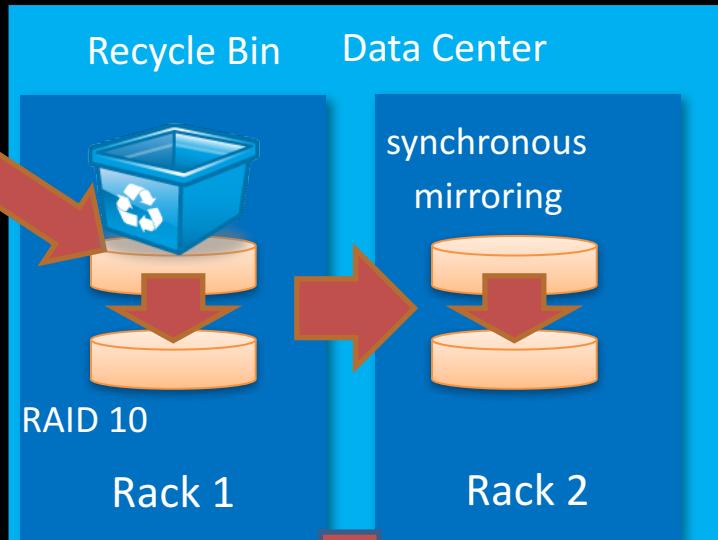
disk

Failure Scope

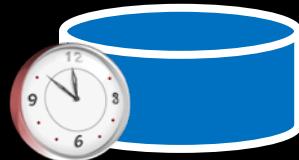
save



client side
cache



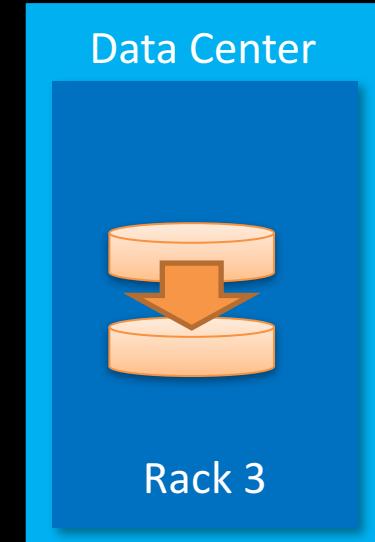
point-in-time
restore



asynchronous
log shipping



asynchronous
replication





Demo: How Forensics is Adapting in the Cloud



Lesson 9 Nuggets of Gold ...

Where do you want (your data) to go today?

Office 365 Exchange Online

My Office 365 organization is hosted by:

Office 365 Worldwide

Office 365 Worldwide

Office 365 China

Office 365 Germany

Office 365 Dedicated



★ [Give Feedback](#)

[back](#)

[next](#)

[cancel](#)

Top Tip: JIT & JEA Come to OneDrive for Business

Share 'EXCHANGE 2013 HYBRID CONFIGURATION WIZARD'

Shared with lots of people

Open to anyone with a guest link

Invite people

Get a link

Shared with

Edit link - no sign-in required

https://ignitetrain.sharepoint.com/_layouts/15/guestaccess.aspx

REMOVE

SET EXPIRATION ▾

- Never
- 1 day
- 30 days
- 60 days
- Custom

Close

Directions: Outlook Anywhere and AutoDiscover. Everything must be working.

Azure Documentation: One Repository to Rule them

The screenshot shows the Microsoft Azure Documentation homepage. At the top, there's a navigation bar with links for "Why Azure?", "Solutions", "Products", "Documentation" (which is highlighted in blue), "Pricing", "Partners", "Blog", "Resources", and "Support". To the right of the navigation are "SALES 0800 098 8435" and "MY ACCOUNT". The main content area has a dark sidebar on the left containing a list of service categories: Overview, Best Practices, Compute, Web & Mobile, Data & Storage, Intelligence, Analytics, Internet of Things, Networking, Media & CDN, Enterprise Integration, Identity & Access Management, Developer Services, Management & Security, and Billing. The "Management & Security" category is also highlighted in blue. The main content area to the right lists several services under "Management & Security": Scheduler (described as running jobs on simple or complex recurring schedules), Operations Management Suite (described as managing and protecting cloud and on-premises infrastructure), Automation (described as simplifying cloud management with process automation), Log Analytics (described as collecting, searching, and visualizing machine data from on-premises and cloud), Key Vault (described as safeguarding and maintaining control of keys and other secrets), Security Center (described as preventing, detecting, and responding to threats with increased visibility), and Security information (described as learning how Azure provides a secure infrastructure for building cloud solutions). A large blue sidebar on the right encourages users to "Sign up for free and get £125 to spend on all Azure services" and includes a "Learn more" link. At the bottom right is a white cloud icon with a blue gear inside.

Microsoft Azure

Why Azure? Solutions Products Documentation Pricing Partners Blog Resources Support

SALES 0800 098 8435 | MY ACCOUNT

Overview

Best Practices

Compute

Web & Mobile

Data & Storage

Intelligence

Analytics

Internet of Things

Networking

Media & CDN

Enterprise Integration

Identity & Access Management

Developer Services

Management & Security

Billing

Management & Security

Scheduler

Run your jobs on simple or complex recurring schedules

Operations Management Suite

Manage and protect your cloud and on-premises infrastructure

Automation

Simplify cloud management with process automation

Log Analytics

Collect, search and visualise machine data from on-premises and cloud

Key Vault

Safeguard and maintain control of keys and other secrets

Security Center

Prevent, detect and respond to threats with increased visibility

Security information

Learn how Azure provides you with a secure infrastructure on which you can build your cloud solutions

Sign up for free and get £125 to spend on all Azure services

Learn more ▶



Incoming: Microsoft Azure Forensics as a Service (FaaS)

Microsoft Azure > Forensics > Settings > Disks

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with icons for NEW, HOME, and NOTIFICATIONS. The main area displays the 'Forensics' virtual machine under the 'RUNNING' section. The 'Capture' button in the VM actions bar is circled in red. To the right, the 'Settings' blade for the 'Forensics' resource group is open, showing options like 'Properties' and 'Scale'. On the far right, the 'Disks' blade is open, listing the 'Forensics' disk with options to 'Attach New...' or 'Attach Existing...'. The overall theme is dark grey.

RUNNING

Forensics
Virtual machine (classic)

Settings Connect Start Restart Shut down Capture Reset Remote... Delete

Essentials

Resource group: Group-1
Status: Running
Location: West US
Subscription name: Visual Studio Ultimate with MSDN

DNS name: forensics-.net
Virtual IP address
Private IP address
Size: Standard A1 (1 Core, 1.75 GB)

Settings

Search settings

Properties Scale

Disks

Forensics

Attach New... Attach Existing...

DISK

OS DISK

Forensics-

DATA DISKS



Lesson 10 All Hail the Azure Security Centre

Azure Security Centre

Explore in Pow...

Prevention

Resource security health

Virtual machines	<div style="width: 100%;"> </div>
Networking	<div style="width: 50%; background-color: #99ff00;"> </div>
SQL	<div style="width: 100%;"> </div>
Applications	<div style="width: 100%;"> </div>

HIGH SEVERITY 11 resources HEALTHY 3 resources

Add tiles

Recommendations

Partner solutions

No solutions

Policy Quickstart

Recommendations

Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	...
Install Endpoint Protection	5 virtual mac...	Open	! High	...
Add a web application firewall	2 web applic...	Open	! High	...
Add a Next Generation Firewall	2 endpoints	Open	! High	...
Enable Network Security Groups on subn...	2 subnets	Open	! High	...
Enable Network Security Groups on virtu...	2 virtual mac...	Open	! High	...
Enable Transparent Data Encryption	2 SQL databa...	Open	! High	...
Apply disk encryption	5 virtual mac...	Open	! High	...
Reboot after system updates	2 virtual mac...	Open	⚠ Medium	...
Provide security contact details	1 subscriptions	Open	⚠ Medium	...

Review

Azure Information Protection

Azure Security Portal

BitLocker Disk Encryption

Azure Security Troubleshooter

Azure Security Documentation

Container Security

Multi Factor Authentication

Azure Forensics

Azure Security Health Monitoring

Azure AD Privileged Identity Management

Azure AD Connect Health

Hybrid Management

Microsoft Anti Malware For Cloud Services & Virtual Machines

Azure Key Vault

Azure AD Identity Protection

Azure Business Continuity



Follow me on Twitter
@AndyMalone



The premium event for IT-professionals

Feb. 1-3rd in Oslo Spektrum
