Microsoft

Azure Government Amendment

Microsoft Services

Agenda

- Overview of the US Government Cloud
- Commercial / US Government Comparison
- Selecting a Cloud and the Trust Center
- Azure Blueprints
- Connecting to the US Government Cloud
- Marketplace Considerations
- Azure Active Directory Considerations
- About the Feature Roadmap
- Useful Links

Microsoft Confidential

Microsoft

Overview of the US Government Cloud

Microsoft Services

What is the US Government Cloud?

"A government-community cloud you can trust, with world-class security and compliance, enabling U.S. government and their partners to transform their mission-critical workloads to the cloud."

Hybrid flexibility		Engineered for flexibility and consistency across public, private, and hosted clouds
Comprehensive compliance		The most certifications of any cloud provider to simplify critical government compliance requirements
Superior protection		Hardened US datacenters, including East coast, with 500-mile geo-redundancy, operated by screened US persons
Government only		Unique cloud instance, exclusively for government customers and their solution providers

Microsoft Confidential

Unique Properties of the US Government Cloud

- Physically isolated instance of Microsoft Azure
- Employs world-class security and compliance services critical to U.S. government for all systems and applications built on its architecture
  - FedRAMP and DoD compliance certifications
  - CJIS state-level attestations
  - Ability to issue HIPAA Business Associate Agreements
  - Support for IRS 1075
- Operated by screened U.S. citizens

Microsoft Confidential

Azure DoD/Government Regions

Microsoft Confidential

Microsoft

Commercial / US Government Comparison

Microsoft Services

Commercial vs. US Government Clouds

Comparison Point	Microsoft Azure Commercial (MAC)	Microsoft Azure Government (MAG)
Operational staff	Microsoft screening	Screened US citizens
Physical security	Biometrics, isolation, fencing, etc.	Same as MAC
Scope of offering	All Azure features	Features limited by certification
Portal (Classic)	https://manage.windowsazure.com	https://manage.windowsazure.us
Portal (ARM)	https://portal.azure.com	https://portal.azure.us
Pricing concerns	Base pricing, minus EA/commitment discount (if any)	Base pricing, plus MAG premium, minus EA/commitment discount (if any)
Availability	Anyone, on demand	Requires approval from Microsoft
Identity (Azure AD)	Integrates Office 365 & 3rd party SaaS	Isolated, no integration

Microsoft Confidential

Microsoft

Selecting a Cloud and the Trust Center

Microsoft Services
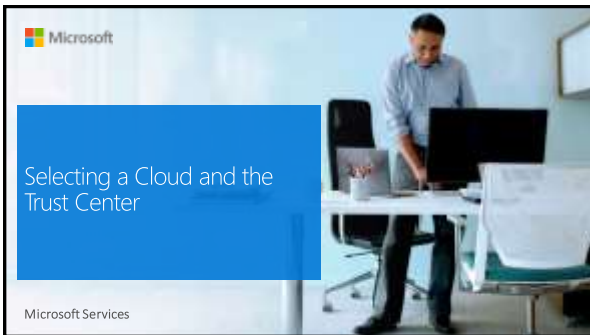
Selecting a Cloud: Why the Government Cloud?

"I'm a Government Entity so obviously, MAG is the way to go!"

- This is inappropriate thinking
- Microsoft Azure Government...
  - Is more expensive due to extra certification requirements and overhead
  - Is slower to gain features due to certification timelines
- Microsoft Azure Commercial...
  - Meets FedRAMP Moderate and many other certifications
  - Has same physical security
- Very common for Government customers to have both MAG and MAC subscriptions
- To compare services available, see https://azure.microsoft.com/en-us/regions/services/

Microsoft Confidential

Azure covers 54 compliance offerings
Azure has the deepest and most comprehensive compliance coverage in the industry

Global	ISO 27001	ISO 27018	ISO 27017	ISO 22301	ISO 9001	SOC 1 Type 2	SOC 2 Type 2	SOC 3	CSA STAR Self-Assessment	CSA STAR Certification	CSA STAR Attestation

US Gov	Moderate JAB P-ATO	High JAB P-ATO	DoD DISA SRG Level 2	DoD DISA SRG Level 4	DoD DISA SRG Level 5	SP 800-171	FIPS 140-2	Section 508 VPAT	ITAR	CJIS	IRS 1075

Industry	PCI DSS Level 1	CDSA	MPAA	FACT UK	Shared Assessments	FISC Japan	HIPAA / HITECH Act	HITRUST	GxP 21 CFR Part 11	MARS-E	IG Toolkit UK	FERPA	GLBA	FFIEC

Regional	Argentina PDPA	EU Model Clauses	UK G-Cloud	China DJCP	China GB 18030	China TRUCS	Singapore MTCS	Australia IRAP/CCSL	New Zealand GCIO	Japan My Number Act	ENISA IAF	Japan CS Mark Gold	Spain ENS	Spain DPA	India MeitY	Canada Privacy Laws	Privacy Shield	Germany IT Grundschutz workbook

---

Commercial vs. US Government Clouds – Compliance Offerings

Comparison Point	Microsoft Azure Commercial (MAC)	Microsoft Azure Government (MAG)
FedRAMP	Moderate	High
US Department of Defense	Level 2 (specific services)	Level 4 (specific services) Level 5 (specific services in DoD regions)
CJIS	N/A	Attestation by State
FIPS 140-2	✔	✔
ITAR	N/A	✔
NIST 800-171	✔	✔
IRS 1075	N/A	✔
HIPAA / HITECH	✔	✔
MARS-E	✔	✔
Section 508	✔	✔
HITRUST	✔	N/A
FERPA	✔	N/A
FDA CFR Title 21 Part 11	✔	N/A
PCI DSS 3.2 SP L1	✔	N/A

The Microsoft Trust Center

The Microsoft Trust Center offers detailed security, privacy, and compliance information for all Microsoft cloud services.

Obtain targeted information based on your role in the organization

- Review by job role
- Review by product/service
- Review by cloud

https://www.microsoft.com/en-us/trustcenter

The Microsoft Trust Center

The Microsoft Trust Center

Scope & filter Microsoft's compliance offerings based on Region, Country, Industry, and Product/Service

Easily determine which Cloud service is best suited for a particular workload

https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

The Microsoft Trust Center

The Microsoft Trust Center

Dive deeper into a compliance offering to see its audit, in-scope services, and how Microsoft ensures ongoing compliance

(CJIS Example)

Microsoft

Azure Blueprints

Microsoft Services

Azure Blueprints

- Purpose
  - Facilitate the secure and compliant use of Azure for government
  - Leverage Azure's FedRAMP JAB Provisional Authority to Operate (P-ATO) or DoD Provisional Authorization (PA)
  - Reduce the scope of customer-responsibility security controls in Azure-based systems
- Customer Responsibilities Matrix (CRM)
  - Lists all NIST SP 800-53 security control requirements for FedRAMP and DISA baselines
- System Security Plan (SSP)
  - Documents both customer security control implementations as well as controls inherited from Azure

Microsoft Confidential

Azure Blueprints – Customer Responsibilities Matrix (CRM)

- Lists all NIST SP 800-53 security control requirements for FedRAMP and DISA baselines

(example of FedRamp Moderate for IaaS)

Customer Responsibility	Controls Reference

Azure Blueprints - System Security Plan (SSP)

- Documents both customer security control implementations as well as controls inherited from Azure

(example of FedRamp Moderate)

Azure Blueprints

- High-level discussion: https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-plan-compliance
- Request the blueprints - AzureBlueprint@microsoft.com

Microsoft Confidential

Microsoft

Connecting to the
US Government Cloud

Microsoft Services

Portal Addresses

Portal	MAC URL	MAG URL
Classic Management	https://manage.windowsazure.com	https://manage.windowsazure.us
ARM Management	https://portal.azure.com	https://portal.azure.us
Enterprise Agreement (EA)	https://ea.azure.com	
Account Management	https://account.windowsazure.com	https://account.windowsazure.us
Operations Management Suite (OMS)	https://mms.microsoft.com	https://oms.microsoft.us

See https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-services

Microsoft Confidential

Connecting with Command Line Interfaces

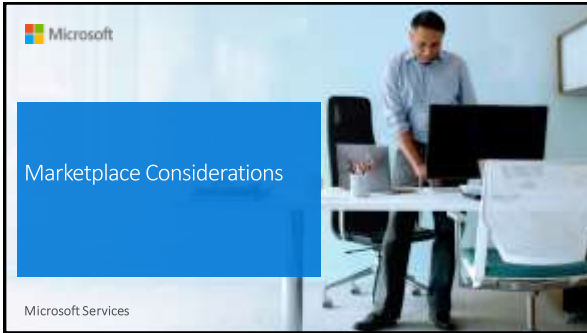| Service	Command
Azure ARM	Add-AzureRmAccount -EnvironmentName AzureUSGovernment
Azure ASM	Add-AzureAccount -Environment AzureUSGovernment
AzureAD ARM	Connect-AzureAD -AzureEnvironmentName AzureUSGovernment
AzureAD ASM	Connect-MsolService -AzureEnvironment UsGovernment
Azure CLI	azure login -environment "AzureUSGovernment"

Microsoft Confidential

Connecting with Visual Studio 2015

- Hardcode the Azure Government endpoints with a registry key
  - Visual Studio can only be used for Azure Government deployments from then on
- Reset the registry key to return connectivity to Commercial endpoints
  - Visual Studio can only be used for Azure Commercial deployments from then on
- https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-get-started-connect-with-vs#visual-studio-2015

Microsoft Confidential

Connecting with Visual Studio 2017

- Hardcode the Azure Government endpoints with a configuration file located in a specific folder
  - Visual Studio can only be used for Azure Government deployments from then on
- Rename or delete the folder to return connectivity to Commercial endpoints
  - Visual Studio can only be used for Azure Commercial deployments from then on
- https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-get-started-connect-with-vs#visual-studio-2017

Microsoft Confidential

Microsoft

Marketplace Considerations

Microsoft Services

Marketplace Considerations

- Similar experience to public Azure portal
- Only BYOL images available (cannot bill through the Marketplace)
- Only a subset of images are available
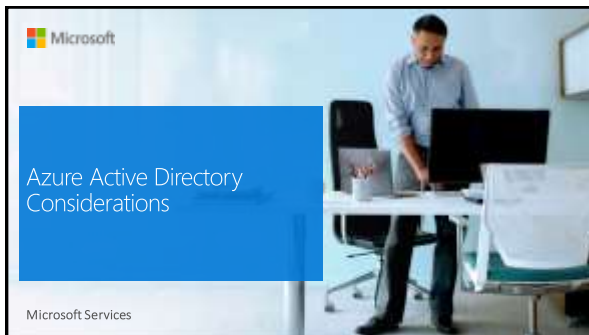- If in an Enterprise Agreement, Marketplace must be enabled in the EA Portal
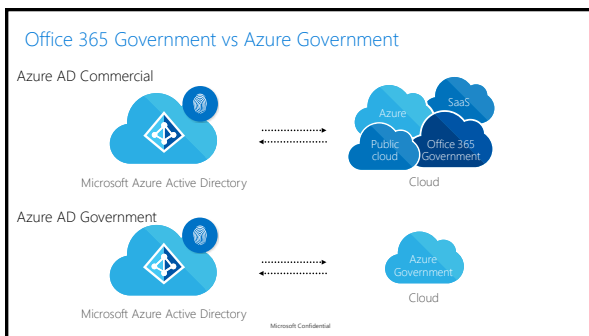
Microsoft Confidential

Bringing Commercial to MAG

How quickly do you need it?

- Immediate need
  - Deploy into an Azure Commercial subscription with same environment setup as intended Government environment (i.e. Network)
  - Copy the VHDs to Azure Government subscription and re-deploy
  - Warning: Offerings not certified for Azure Government may not work or be supported
  - The vendor can also privately grant access to the solution through alternate means
- Wait and Certify
  - Ask the vendor to follow the publishing guidelines for Azure Government Marketplace
  - This ensures the offering meets the standards for the Marketplace. (Support, Compatibility, etc)

Microsoft Confidential

Azure Active Directory
Considerations

Microsoft Services

Office 365 Government vs Azure Government

Azure AD Commercial

Microsoft Azure Active Directory

Cloud

Azure AD Government

Microsoft Azure Active Directory

Cloud

Azure AD Commercial vs Azure AD Government

- Completely independent instances of the Azure AD (AAD) service
- An on-premises identity can only be synced to 1 AAD tenant (i.e. John@contoso.com)
  - It is unsupported to sync the same identity to more than 1 AAD tenant
  - Workaround: Create a new on-premises identity for the other AAD tenant
- AAD Commercial works with O365 Commercial/Government, 3rd party SaaS, and identity enhancement services
  - Enterprise Mobility and Security (EMS), AAD Premium, Identity Protection, Privileged Identity Management
- AAD Government only integrates with AAD Application Proxy (publishing on-premises web/thick solutions)
  - AAD Premium (est. June 2017)

Microsoft

About the Feature Roadmap

Microsoft Services

Roadmap Concepts

- The Azure Government team has a product roadmap
- Generally updated monthly
- Includes what's live and what's coming
- Includes anticipated timeframes
- Includes compliance offering expectations (e. g. CJIS state-by-state information)
- Often issued in PowerPoint and Word forms
- Covered under the NDA between the customer and Microsoft

Microsoft Confidential

How to Get It

- Available via your Microsoft account team

Microsoft Confidential

Microsoft

Useful Links

Microsoft Services

References

- Azure Government Blog – https://blogs.msdn.microsoft.com/azuregov/
  - Announces new feature releases and blogs specific to working with MAG
- Azure Government Documentation - https://docs.microsoft.com/en-us/azure/azure-government/
  - Includes feature availability and details on difference between MAC and MAG versions of the offering
- Features Available Region - https://azure.microsoft.com/en-us/regions/services/
  - "Get-AzureRMLocation" in Powershell to see a real-time listing of VM sizes, storage, etc. available in each region

---

Microsoft