

---

# Deployment, Security, and Cloud Management



DSBA 6190-U90 | Colby T. Ford, Ph.D.

---

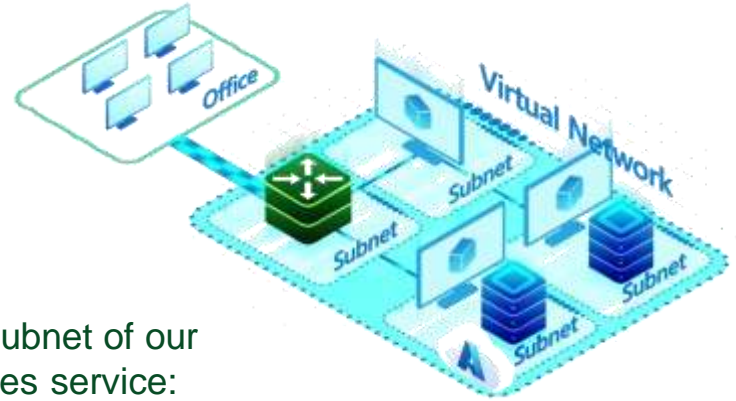
# Deploying Azure Resources

- Basics of Networking
  - Infrastructure as Code
    - ARMs and Biceps
    - Terraform
  - GitHub Actions / DevOps Build Pipelines
-

---

# Networking

# Virtual Networks and Subnets

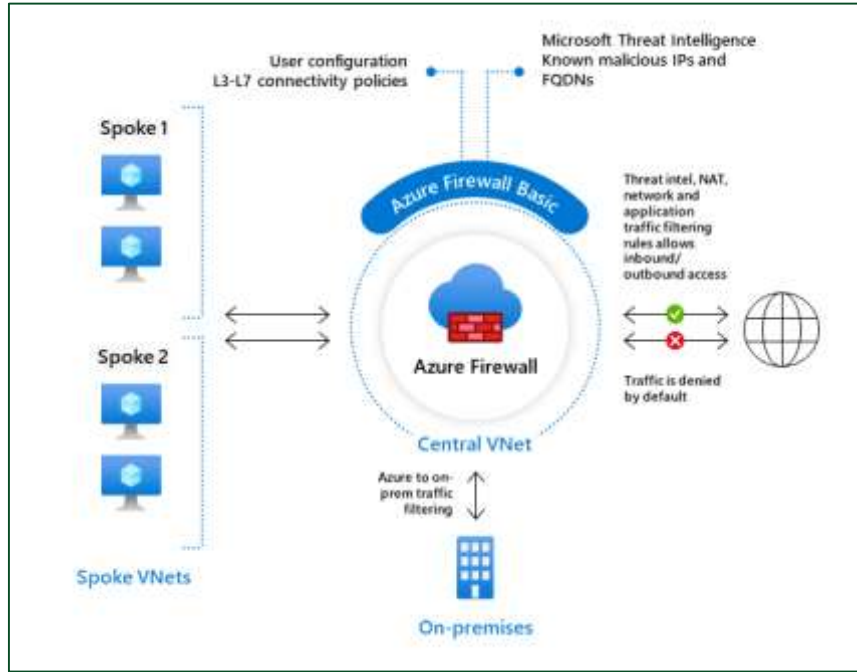


Example: the subnet of our class Kubernetes service:

- Virtual networks, like real networks, control the communication between cloud services, the internet, and on-prem resources
- Other features:
  - Control and filter internet vs. internal routing
  - DDoS protection
  - Network Peering
- Subnets relate to a specific service, giving an address space to each (CIDR block)

Subnet ID	/subscriptions/e9bc187a-e9a1-46be-822e-e955a2563601/resourceG
Subnet purpose ⓘ	Default
Name * ⓘ	aks-subnet
<b>IPv4</b>	
Include an IPv4 address space	<input checked="" type="checkbox"/>
Choose a starting address and size within your IPv4 address range: 10.224.0.0/12 (10.224.0.0 - 10.239.255.255)	
Starting address * ⓘ	10.224.0.0
Size ⓘ	/16 (65,536 addresses)
Subnet address range ⓘ	10.224.0.0 - 10.224.255.255

# Firewalls and Private Endpoints



## Firewalls:

- Firewalls allow you to communicate with multiple networks (including virtual networks) and control access (certain IPs, ports, etc.)
- Also, it provides some enhanced threat detection, and traffic filtering, etc.

## Private Endpoints:

- Normally, Azure services have a public endpoint (a public URL where you can access the service from the open internet). For security reasons, you can make an endpoint for certain services as part of your vnet.

# Infrastructure-as-Code

---

# Deployment is ~~Easy~~ Necessary

- “Infrastructure as Code” – The ability to deploy all your services in the cloud from code rather than manually.
  - Important for:
    - IT management of resources
    - Geo-replication / Global availability and scale
    - Security
    - Promotion of infrastructure changes from:  
development → staging → production
-

---

# Infrastructure as Code Options



ARM Templates

Pro: Azure can generate them.

Con: Difficult to read and edit.

[Templates overview -  
Azure Resource Manager  
| Microsoft Docs](#)



Bicep Language

Pro: From Microsoft. Easy to read.

Con: Lacking in examples and docs.

[Bicep language for deploying  
Azure resources - Azure  
Resource Manager | Microsoft  
Docs](#)



Terraform

Pro: From HashiCorp. Multicloud.

Con: Proprietary and Pricey

[Docs overview |  
hashicorp/azurerm | Terraform  
Registry](#)

---



# IaC Language Learning Curve

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "location": {
      "type": "string",
      "defaultValue": "[resourceGroup().location]"
    },
    "storageAccountName": {
      "type": "string",
      "defaultValue": "[format(myStorage{0}',
uniqueString(resourceGroup().id))]"
    }
  },
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2021-06-01",
      "name": "[parameters('storageAccountName')]",
      "location": "[parameters('location')]",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "StorageV2",
      "properties": {
        "accessTier": "Hot"
      }
    }
  ]
}
```

**ARM (JSON)**

```
param location string = resourceGroup().location
param storageAccountName string =
myStorage${uniqueString(resourceGroup().id)}

resource storageAccount
'Microsoft.Storage/storageAccounts@2021-06-01' = {
  name: storageAccountName
  location: location
  sku: {
    name: 'Standard_LRS'
  }
  kind: 'StorageV2'
  properties: {
    accessTier: 'Hot'
  }
}
```

**BICEP**

```
resource "azurerm_storage_account" "mystorage" {
  name = "myStorage${random_integer.id.result}"
  resource_group_name = azurerm_resource_group.rg.name
  location = azurerm_resource_group.rg.location
  account_tier = "Standard"
  account_replication_type = "LRS"
  tags = { environment = "dev" }
}
```

**TF (HCL)**

# Service Principals and Managed Identities

- Service Principals are like user accounts, but for services.
  - “Azure-representation of a non-Azure object”
  - Usually assigned for a specific application or purpose.
- Managed Identities are a type of Service Principal that operates on behalf of other services (usually other Azure resources)
  - System-assigned managed identities share a lifecycle with various Azure services
- Both can be given roles and permissions like users.

## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

### Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (ONIDC only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

Subscription ID \*

DSI-23950 Subscription (e9bc187a-e9a1-46be-822e-e955a2563601)

Storage account \*

stod2ba6190class (rg-dsba6190-class-dev-eastus-001)

Blob container \*

datalake

☒ Save credentials with the datastore for data access ⓘ

Authentication type \* ⓘ

Account key ⓘ

Account key \* ⓘ

☒ Use workspace managed identity for data preview and profiling in Azure Machine Learning studio ⓘ

ⓘ Warning: We could not verify whether the workspace managed identity has sufficient permissions on the resource to enable data access. ⓘ [More details](#)

## Managed Identities

University of North Carolina at Charlotte (student.uncc.edu)

[+ Create](#)
[Manage view](#)
[Refresh](#)
[Export to CSV](#)
[Open query](#)
[Assign tags](#)
[Delete](#)

Subscription equals all
Resource group equals all
Location equals all
[Add filter](#)

Showing 1 to 2 of 2 records.

<input type="checkbox"/> Name	Type	Resource group	Location
<input type="checkbox"/> kub-dsba6190-class-dev-eastus-001-agentpool	Managed Identity	MC_rg-dsba6190-class-dev-eastus-001_kub-ds-	East US
<input type="checkbox"/> dbmanagedidentity	Managed Identity	mrg-dsba6190-class-dev-eastus-001	East US

```
{
  "appId": "c075ec05-db99-4195-ba8b-f0d42995e5e1",
  "displayName": "dsba6190devops",
  "password": "Pw00t@-4uT4Zv91,11B0Q000u,agp0Q0u0-gi4b4v",
  "tenant": "88d59d7d-aecb-41b2-90c5-55595de02536"
}
```

---

# Deploying with GitHub Actions

# Steps to Deploy with Terraform in GitHub Actions

Make GitHub Repo



Add Cloud Secrets to Repo



Add YAML file to .github/actions folder



Add Terraform File(s) to Repo



Commit and Push Changes to Repo

# Security, Compliance, and Data Governance

- Role-Based Access Controls
    - Azure Active Directory
    - Access Control Lists in Azure Storage
  - Compliance
    - HIPAA, HITRUST, SOX, ISO
    - Defender for Cloud
    - Blueprints, etc.
  - And more...
    - Data Governance: Azure Purview
    - Azure Chaos Studio
    - Subscriptions
-



# Azure Active Directory (Entra ID)

- Identity management for users and applications.
  - Single Sign-On (SSO)
  - App registrations
    - External applications
    - Service Principals and Managed Identities
  - Role assignments
  - Group organization

The screenshot displays the Microsoft Azure portal interface for the University of North Carolina at Charlotte's Azure Active Directory (Entra ID) tenant. The top navigation bar includes the Microsoft Azure logo and a search bar. The main header shows the tenant name and "Overview". The left sidebar contains a navigation menu with options like Overview, Preview features, Diagnose and solve problems, Manage, Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Custom security attributes (Preview), Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, and User settings. The main content area shows the "Overview" tab with a search bar for tenants. Below this, the "Basic information" section displays key tenant details in a table:

Basic information	
Name	University of North Carolina at Charlotte
Tenant ID	e7c4732a-8eba-4356-abd3-18c1dd55004a
Primary domain	student.uncc.edu
License	Azure AD Premium P2

Additional statistics are shown on the right:

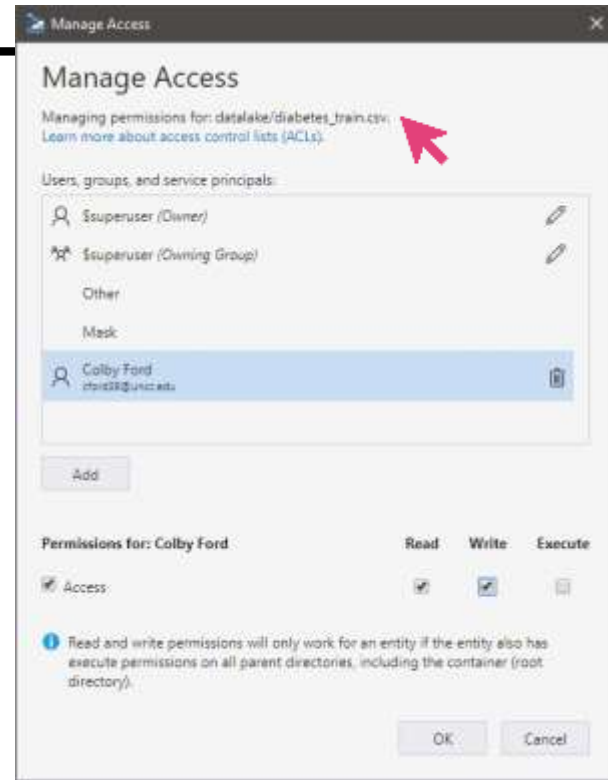
- Users: 11,530
- Groups: 7,800
- Applications: 729
- Devices: 17,760

Below the basic information, there is an "Alerts" section with a warning about "Upcoming TLS 1.0, 1.1 and 3DES deprecation" and a "My feed" section showing a user profile for Colby Ford. A sidebar on the right highlights "Azure AD Connect" as "Enabled" with a "Go to Azure AD Connect" link.

# RBAC and Access Control Lists

- Common Role-Based Access Controls:
  - Owner
    - Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
  - Contributor
    - Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC
  - Reader
    - View all resources but does not allow you to make any changes.

- RBAC: Broad Access to Resources



- ACLs: Finer Access to Data

# Compliance

noun - com·pli·ance | \ kəm-'plī-ən(t)s \

“Conformity in fulfilling  
official requirements”



<b>Global</b> <a href="#">CIS benchmark</a> <a href="#">CSA STAR Attestation</a> <a href="#">CSA STAR Certification</a> <a href="#">CSA STAR self-assessment</a> <a href="#">SOC 1</a> <a href="#">SOC 2</a> <a href="#">SOC 3</a> <a href="#">ISO 20000-1</a> <a href="#">ISO 22301</a> <a href="#">ISO 27001</a> <a href="#">ISO 27017</a> <a href="#">ISO 27018</a> <a href="#">ISO 27701</a> <a href="#">ISO 9001</a> <a href="#">WCAG</a>	<b>US government</b> <a href="#">CJIS</a> <a href="#">CMMC</a> <a href="#">CNSSI 1253</a> <a href="#">DFARS</a> <a href="#">DoD IL2</a> <a href="#">DoD IL4</a> <a href="#">DoD IL5</a> <a href="#">DoD IL6</a> <a href="#">DoE 10 CFR Part 810</a> <a href="#">EAR</a> <a href="#">FedRAMP</a> <a href="#">FIPS 140</a> <a href="#">ICD 503</a> <a href="#">IRS 1075</a> <a href="#">ITAR</a> <a href="#">JSIG</a> <a href="#">NDAA</a> <a href="#">NIST 800-161</a> <a href="#">NIST 800-171</a> <a href="#">NIST 800-53</a> <a href="#">NIST 800-63</a> <a href="#">NIST CSF</a> <a href="#">Section 508 VPATs</a> <a href="#">StateRAMP</a>	<b>Financial services</b> <a href="#">23 NYCRR Part 500 (US)</a> <a href="#">AFM and DNB (Netherlands)</a> <a href="#">AMF and ACPR (France)</a> <a href="#">APRA (Australia)</a> <a href="#">CFTC 1.31 (US)</a> <a href="#">EBA (EU)</a> <a href="#">FCA and PRA (UK)</a> <a href="#">FFIEC (US)</a> <a href="#">FINMA (Switzerland)</a> <a href="#">FINRA 4511 (US)</a> <a href="#">FISC (Japan)</a> <a href="#">FSA (Denmark)</a> <a href="#">GLBA (US)</a> <a href="#">KNF (Poland)</a> <a href="#">MAS and ABS (Singapore)</a> <a href="#">NBB and FSMA (Belgium)</a> <a href="#">OSFI (Canada)</a> <a href="#">OSPAR (Singapore)</a> <a href="#">PCI 3DS</a> <a href="#">PCI DSS</a> <a href="#">RBI and IRDAI (India)</a> <a href="#">SEC 17a-4 (US)</a> <a href="#">SEC Regulation SCI (US)</a> <a href="#">SOX (US)</a> <a href="#">TruSight</a>	<b>Automotive, education, energy, media, and telecommunication</b> <a href="#">CDSA</a> <a href="#">DPP (UK)</a> <a href="#">FACT (UK)</a> <a href="#">FERPA (US)</a> <a href="#">MPA</a> <a href="#">GSMA</a> <a href="#">NERC (US)</a> <a href="#">TISAX</a>
<b>Healthcare and life sciences</b> <a href="#">ASIP HDS (France)</a> <a href="#">EPCS (US)</a> <a href="#">GxP (FDA 21 CFR Part 11)</a> <a href="#">HIPAA (US)</a> <a href="#">HITRUST</a> <a href="#">MARS-E (US)</a> <a href="#">NEN 7510 (Netherlands)</a>			<div> <b>Regional - Americas</b>  <a href="#">Argentina PDPA</a>  <a href="#">Canada privacy laws</a>  <a href="#">Canada Protected B</a>  <a href="#">US CCPA</a> </div> <div> <b>Regional - Asia Pacific</b>  <a href="#">Australia IRAP</a>  <a href="#">China GB 18030</a>  <a href="#">China DJCP (MLPS)</a>  <a href="#">China TCS</a>  <a href="#">India MeitY</a>  <a href="#">Japan CS Gold Mark</a>  <a href="#">Japan ISMAP</a>  <a href="#">Japan My Number Act</a>  <a href="#">Korea K-ISMS</a>  <a href="#">New Zealand ISPC</a>  <a href="#">Singapore MTCS</a> </div> <div> <b>Regional - EMEA</b>  <a href="#">EU Cloud CoC</a>  <a href="#">EU EN 301 549</a>  <a href="#">ENISA IAF</a>  <a href="#">EU GDPR</a>  <a href="#">EU Model Clauses</a>  <a href="#">Germany C5</a>  <a href="#">Germany IT-</a>  <a href="#">Grundschutz workbook</a>  <a href="#">Netherlands BIR 2012</a>  <a href="#">Russia personal data law</a>  <a href="#">Spain ENS High</a>  <a href="#">Spain LOPD</a>  <a href="#">UAE DESC</a>  <a href="#">UK Cyber Essentials Plus</a>  <a href="#">UK G-Cloud</a>  <a href="#">UK PASF</a> </div>
<b>Azure Compliance Offerings</b>			

# HIPAA, HITECH, and HITRUST

- **HIPAA:** Health Insurance Portability and Accountability Act of 1996
  - Sets requirements for using, disclosing, and handling protected health information (PHI)
- **HITECH:** Health Information Technology for Economic and Clinical Health Act of 2009
  - Extends HIPAA for electronic health records and more modern, data-driven technology in healthcare
- **HITRUST:** Health Information Trust Alliance
  - A private company that sets standards, based on HIPAA/HITECH, and provides certification.



Name	Address (Smaller than first 3 digits of zip code)	Dates (Smaller than years)
Telephone Number	Fax Number	Email Address
Social Security Number	Medical Record Number	Health Plan Beneficiary Number
Account Numbers	License Number	Vehicle Identifiers
Device Identifiers and Serial Numbers	Web URLs	IP Addresses
Biometric Identifiers • Fingerprints, voice recording, etc.	Face Photos	Any other unique ID

# SOX

- Sarbanes-Oxley Act of 2002
  - US federal law from the Securities and Exchange Commission (SEC)
  - Mandates financial record keeping practices
  - Thanks to the ENRON and WorldCom scandals

Retain data for the req'd amount of time

- Offsite backups

Manage security and access controls

- Physical and electronic access

Know when something is deleted or changed (version control)

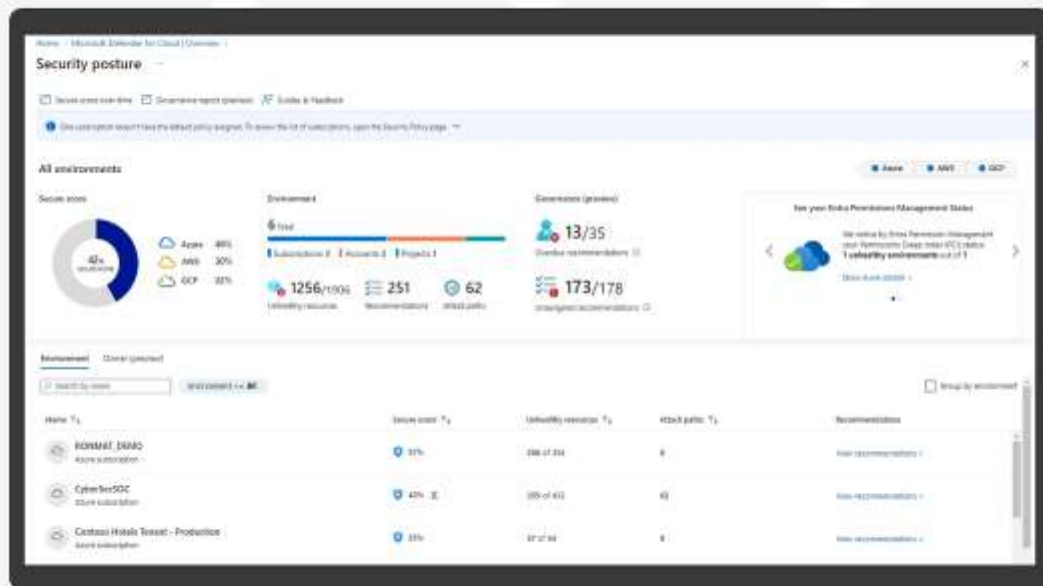
- Prevent data tampering
- Audit trails, logs

Prove you've retained compliance for a rolling 90 days

- Visibility into system and org compliance



- | Total: 49 resources                |          |                                |
|------------------------------------|----------|--------------------------------|
| 49 Defender CSPM Resources         | \$5      | Virtual resource/Month         |
| 0 Servers (Plan 2)                 | \$15     | Servers/Month                  |
| 0 App Service Instances            | \$15     | Instances/Month                |
| 19 Azure SQL Databases             | \$15     | Servers/Month                  |
| 0 SQL servers on machines          | \$15     | Servers/Month                  |
|                                    | \$0.015  | Conc/Hour                      |
| 0 Open-source relational databases | \$15     | Servers/Month                  |
| 30 Storage accounts                | \$10     | Storage accounts/Month         |
|                                    | \$0.15   | GB scanned (Software Scanning) |
| 0 Azure Cosmos DB accounts         | \$0.0012 | 100RU/s per hour               |





# Azure Blueprints


- Set of organizational standards and requirements for compliance or policy adherence.
- Orchestrate the deployment of artifacts:
  - Role Assignments
  - Policy Assignments
  - Azure Resource Manager templates (ARM templates)
  - Resource Groups

Alt services > Blueprints >

## Create blueprint
















Choose a blueprint sample

You can start with a blank blueprint or pick one of our pre-defined samples to help you get started quickly.

**Blank Blueprint**  
An empty blueprint with no initial properties or artifacts.  
[Start with blank blueprint](#)

### Other Samples

Filter samples by name and description

Name	Description
 Australian Government ISM PROTECTED	Deploys and configures policies mapped to specific Australian Government Information Security Manual (ISM) ...
 Azure Security Benchmark Foundation L...	Deploys and configures Azure Security Benchmark Foundation (Preview). <a href="#">Learn more</a>
 Basic Networking (VNET)	Configures a virtual network with a subnet and an NSG.
 CAF Foundation	Microsoft Cloud Adoption Framework for Azure - Configure Foundational best practices <a href="#">Learn more</a>
 CAF Migration landing zone	Microsoft Cloud Adoption Framework for Azure - Migrations landing zone <a href="#">Learn more</a>
 Canada Federal FIMM	Assigns policies to address Canada Federal FIMM controls. <a href="#">Learn more</a>
 Common Policies	A set of popular policies to apply to a subscription.
 ISO 27001	Assigns policies to address specific ISO 27001:2013 controls. <a href="#">Learn more</a>
 ISO 27001: ASE/SQL Workload	Deploys and configures Azure App Service and SQL DB. Extends ISO Shared Service Blueprint. <a href="#">Learn more</a>
 ISO 27001: Shared Services	Deploys and configures Azure infrastructure and policies mapped to specific ISO controls. <a href="#">Learn more</a>
 New Zealand Information Security Man...	Assigns policies to address specific New Zealand Information Security Manual controls <a href="#">Learn more</a>
 Resource Groups with RBAC	Sets up two resource groups and configures a role assignment for each. <a href="#">Learn more</a>
 SWIFT CSP-CSCF v2020	Assigns policies to address specific SWIFT CSP-CSCF v2020 controls. <a href="#">Learn more</a>
 UK OFFICIAL	Deploys and configures policies mapped to specific UK OFFICIAL controls. <a href="#">Learn more</a>
 UK NHS	Deploys and configures policies mapped to specific UK NHS controls. <a href="#">Learn more</a>

# ISO 27001

- International Standard for *information security*
- 14 main Controls
  - Information security policies, HR security, asset management, access control, cryptography, physical security, etc.

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name
Subscription
<input type="checkbox"/> [Preview]: Deploy Log Analytics Agent for Linux VMs
<input type="checkbox"/> [Preview]: Deploy Log Analytics Agent for Windows VMs
<input type="checkbox"/> [Preview]: Deploy Log Analytics Agent for Windows VM Scale Sets (VMSS)
<input type="checkbox"/> [Preview]: Deploy Log Analytics Agent for Linux VM Scale Sets (VMSS)
<input type="checkbox"/> ISO 27001:2013
<input type="checkbox"/> Allowed locations
<input type="checkbox"/> Allowed locations for resource groups
<input type="checkbox"/> Allowed storage account SKUs
<input type="checkbox"/> Allowed virtual machine SKUs
<input type="checkbox"/> Deploy default Microsoft IaaSAntimalware extension for Windows Server
<input type="checkbox"/> Deploy network watcher when virtual networks are created
<input type="checkbox"/> Deploy SQL DB transparent data encryption
<input type="checkbox"/> Deploy Threat Detection on SQL servers
<input type="checkbox"/> Enforce automatic OS upgrade with app health checks on VMSS
<input type="checkbox"/> Enforce encryption on Data Lake Store accounts
+ Add artifact...



## Add artifact

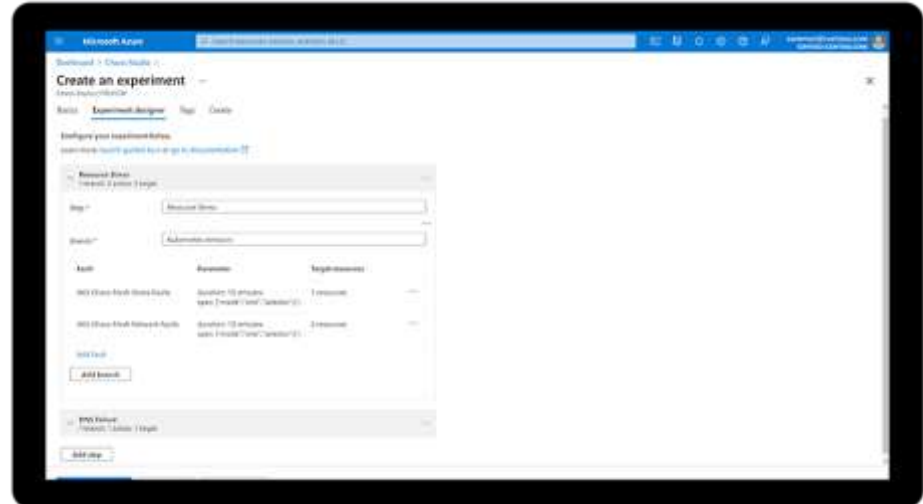
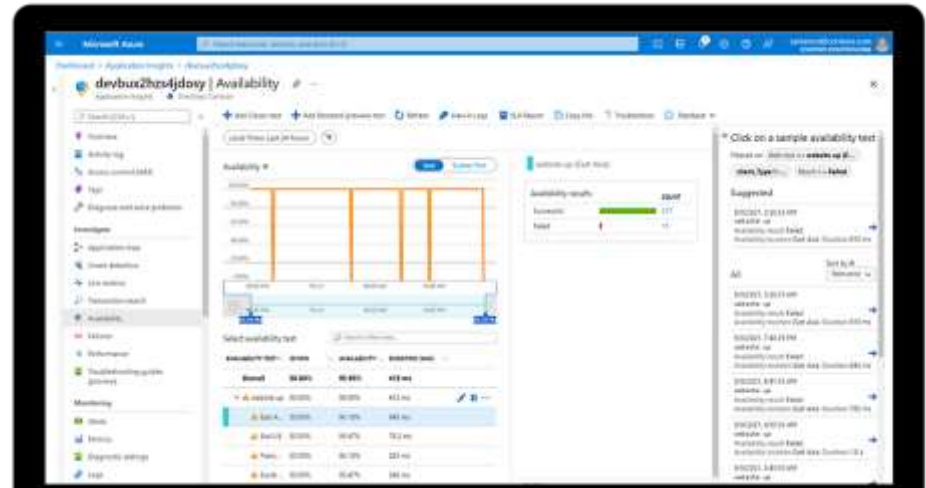
Artifact type \*

- Policy assignment
- Role assignment
- Azure Resource Manager template (Subscription)
- Resource group



# Azure Chaos Studio

- Run experiments to see how your infrastructure handles certain scenarios
  - Disaster recovery
  - Fault injections
  - Code optimizations



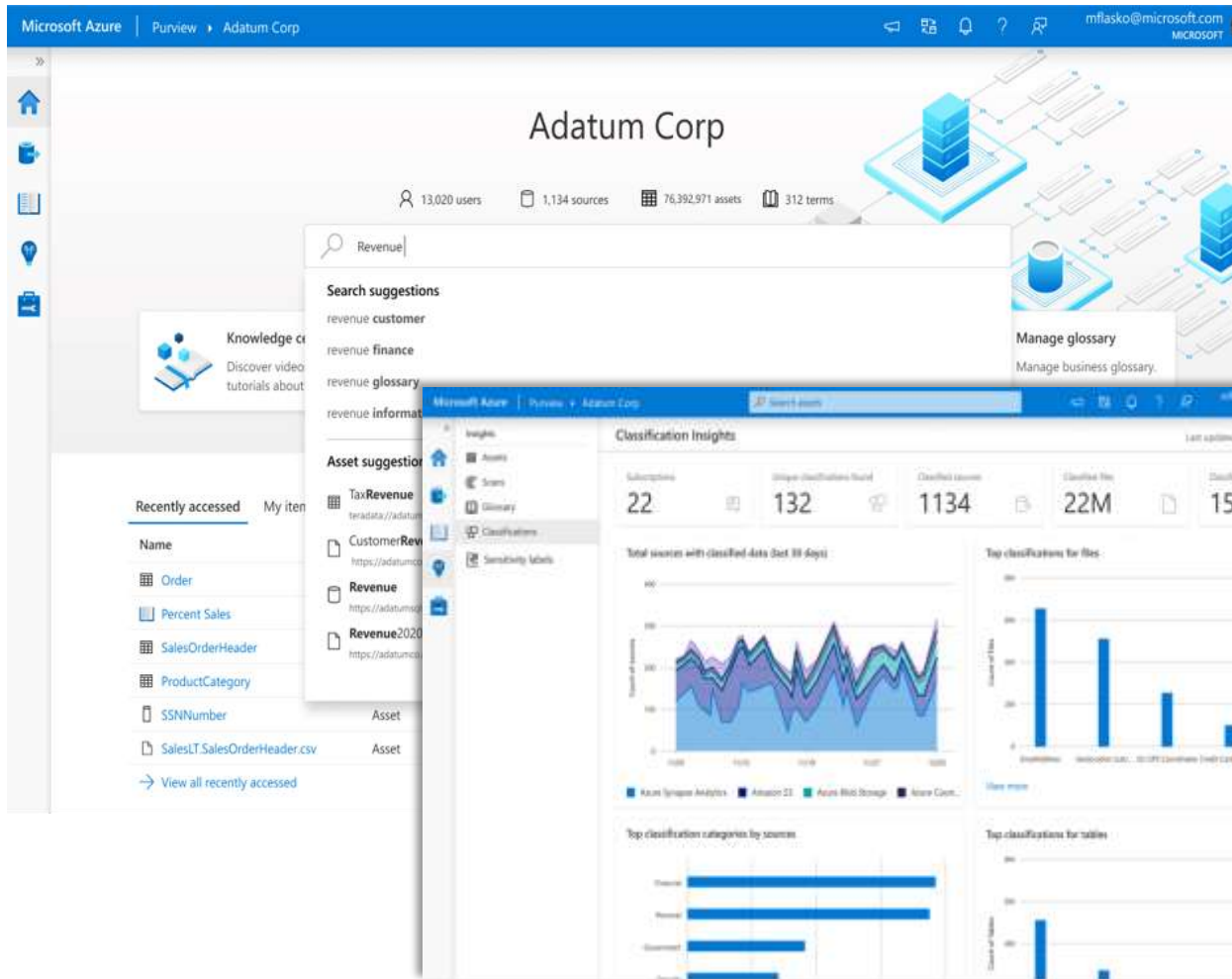
---

**Now that I have a  
bunch of stuff in the  
cloud, how do I see  
it all?**



# Azure Purview





- Data governance platform in Azure that allows us to manage on-prem and multicloud data and services.
  - Create a map of your data estate – “Data Catalog”
  - Find, label, and track sensitive data.
  - See how data flows through your platforms





Showing 5 collections, 1134 sources



Map view


NorthAmericaDataCenter  
Collection










 OnPremSQLServer-Fina...  
SQL Server


 [View details](#)



 Teradata-FinanceData  
Teradata (Preview)


 [View details](#)



 HiveMetastore  
Hive Metastore (Preview)


 [View details](#)



 FinanceSQLServer  
SQL Server

 [View details](#)





 Teradata  
Teradata (Preview)


 [View details](#)


 OnPremSQLServer  
SQL Server






EuropeDataCenter  
Collection










 SAP-S4HANA-Procurem...  
SAP S/4Hana (Preview)


 [View details](#)



 SAP-ECC-SalesData  
SAP ECC (Preview)

 [View details](#)





 SAP-S4HANA  
SAP S/4Hana (Preview)


 [View details](#)


 SAP-ECC  
SAP ECC (Preview)



 [View details](#)


AzureAndBINorthAmerica  
Collection










 AzureDataLakeStorage-...  
Azure Data Lake Storage Gen2


 [View details](#)



 AzureBlobStorage  
Azure Blob Storage


 [View details](#)



 AzureSQLDB-SalesInvoi...  
Azure SQL Database


 [View details](#)



 RevenuePBIDashboards  
Power BI

 [View details](#)





 WebLogs  
Azure Files


 [View details](#)


 AzureSqlManagedInsta...  
Azure SQL Database Managed Instance






AmazonNorthAmerica  
Collection











 AmazonS3-HRData  
Amazon S3


 [View details](#)


 AWS3  
Amazon S3



 [View details](#)

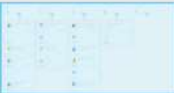
AzureEurope  
Collection





 AzureDataLakeStorage-...  
Azure Data Lake Storage Gen2

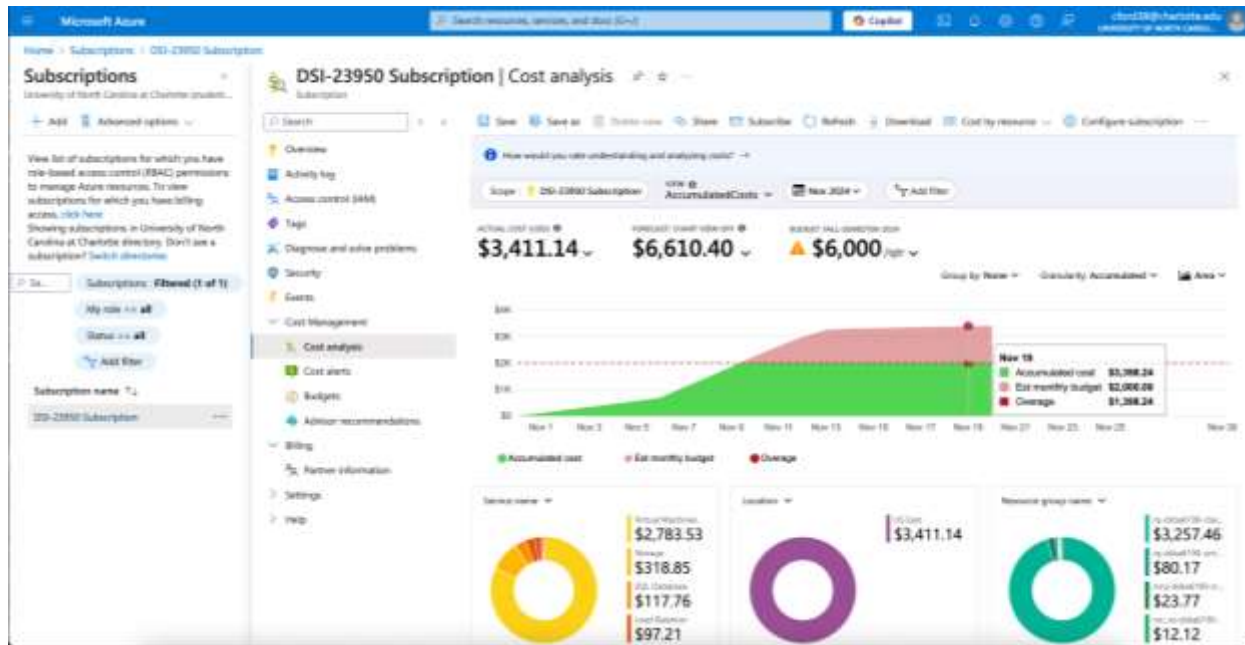
 [View details](#)





# Subscriptions

- Subscriptions are the place where cloud services are billed
- In smaller organizations, it's common to see a single Subscription for the whole company
- In larger organizations, you may see Subscriptions set up for individual groups or applications
  - Also, maybe even separate Subs for dev, staging, and production.



- There are different “offer types” that may affect pricing.
  - Pay-as-you-Go vs. Enterprise Agreement

<https://azure.microsoft.com/en-us/support/legal/offer-details>