AZURE GOVERNANCE FRAMEWORK

Table of Contents

1. Revision History

Revision	Change Description	Updated By	Date
1.0	Developed the document in draft form and presented resource hierarchy to Tyrone Benson and Ian Sanford for review.	James Subido	Jan 22, 2021
2.0	Developed naming convention standards.	James Subido	Feb 4, 2021
3.0	Developed tagging standards.	James Subido	Feb 6, 2021
4.0	Presented this document to Tyrone Benson and Colin Weiner (Microsoft Governance Workshop instructor) for feedback. Updated this document to reflect recommended changes.	James Subido	Feb 10, 2021
5.0	Added RBAC, Entitlement Management, Resource Locks, Cost Management sections and submitted to Tyrone Benson for review.	James Subido	Feb 26, 2021

6.0	Added Azure Tools for Governance, Policy, Monitoring and Alerting, and Blueprints sections.	James Subido	March 4, 2021
7.0	Developed a project plan (*Chapter 17: How do we move forward?*) and submitted to Tyrone Benson, Ian Sanford, Andy Wu, and Wing Chu for review.	James Subido	March 5, 2021
8.0	Updated the document to reflect feedback from Andy Wu. Added *Chapter 5 Risk Assessment* and *Logging and Retention Strategy for Azure Platform Logs* section in Chapter 17. Added Azure AD group naming convention for RBAC delegation.	James Subido	March 25, 2021
9.0	Changed the document to reflect feedback from Tyrone Benson and the Databricks EODS team (ADSB CHSI Program). Added *Chapter 2: CDPH Management Approval* section.	James Subido	April 7, 2021
10.0	Updated the document to reflect changes from EODS Meeting of April 7, 2021: 1) Change wording from "project" to "programs" 2) Categorized Risk Assessment into Cloud Adoption Framework disciplines; 3) Identified various EODS projects as deployable within same subscription (Chapter 8: Subscription Planning section).	James Subido	April 9, 2021
11.0	Updated the document to reflect changes from April 12, 2021, meeting with Tyrone Benson and Andy Wu on Azure RBAC AD Groups and Hub and Spoke Network design. Document to be released for immediate use by SOSS Team (naming conventions) while awaiting signatures from management.	James Subido	April 13, 2021
12.0	Corrected typos and formatting issues and submitted to CDPH Management for signatures.	James Subido	April 20, 2021
13.0	Added a section "Spoke Network Address Space Allocation Planning" section based on feedback from CDPH Weekly Azure Working Session with Microsoft Azure experts.	James Subido	April 27, 2021
14.0	Added to Chapter 9: Naming Conventions: Defined a governance naming convention cut-off date of April 29, 2021, for exemptions. In other words, only Azure resources and	James Subido	April 29, 2021

	services created after April 29, 2021, will need to adhere to the naming conventions. (EODS Meeting of 2021-4-29)		
15.0	Updated the document to reflect changes from CDPH Weekly Azure Working Session with Microsoft Azure experts on April 30 to discuss feedback on this governance document as a whole and May 3 specifically to discuss Cost Management chapter and CDT invoices.	James Subido	May 5, 2021
16.0	Per discussion with Richard Cabutage, allocate an address space of 10.112.0.0/12 which yields 16 subnets and 1,048,574 hosts per subnet for all Azure resources. Allocate 10.127.192.0/18 for core hub and a /18 for all spokes. Summarization of CDPH on-prem resources at 10.226.0.0/15 and 10.228.0.0/14. Updated network design section accordingly.	James Subido	May 24, 2021
17.0	Revised Hybrid Datacenter Architecture. Elaborated on public IP address naming convention.	James Subido	2021-6-4
18.0	With input from Andy and Tyrone, developed a naming convention for Enterprise Applications and the RBAC groups used for administrative delegation leveraging GDSP SIS' Power Platform / Dynamics as a template.	James Subido	2021-6-18
19.0	Document officially adopted during June 23, 2021, meeting. Removed "Draft" watermark and removed "proposed" verbiage.	James Subido	2021-6-23
20.0	Collaborated with Tek Yantra (CAIR2 DVR Project) to develop vNet and subnet naming conventions Updated Resource Hierarchy to reflect changes to Immunization Branch CAIR2 DVR and ESS Landing Zone. Updated Hub and Spoke design to reflect Immunization Branch CAIR2 deployment.	James Subido	2021-7-19
21.0	Added Palo Alto Firewall architectural diagram USWest2.	James Subido	2021-8-11

	Added Appendix A: Naming Convention Cheat Sheet		
22.0	Subnet naming convention: Added host types to conform to established on-prem standards for N-Tier Architecture: USER and DATA. Added Key Vault naming convention on 2021-9-21.	James Subido	2021-9-21
23.0	Custom role based on Contributor built-in role that removes access to the following network components: * VNets * Network Security Groups * Route Tables New standard subnet size: /29 to reduce wasted IP addresses and take into account subnet delegations. Updated RBAC Azure AD Group naming convention to include Access Package Catalogs. Mentioned use of Blueprints for GDSP SIS 2.0 deployment. Documented the procedure for creating Access Packages for Snowflake.	James Subido	2021-12-15
24.0	Added naming convention for Service Accounts and Enterprise Apps	James Subido	2022-1-12
25.0	Introduced the PAM Security Standard section authored by Cannic Hung of the Information Security Office.	James Subido	20223-3-29
26.0	Updated RBAC Scoping authored by Shayaan Motamedi on page 104.	James Subido	2023-7-10

2. Governance Framework Approved by CDPH Management

According to the IT Governance Institute,

> *"IT governance is the responsibility of executives and the board of directors, and consists of leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives."*

As governance starts at the top with leadership, we have the following signatories who have reviewed the governance framework in this document and authorizes its implementation:

Name	Title	Approval Date
John Roussel	Assistant Deputy Director and Chief Technology Officer	June 23, 2021
David Fisher	Chief of ADSB (Application Development and Support Branch)	June 23, 2021
Tony Tran	Chief of DCOSB (Data Center Operations Support Branch)	May 25, 2021
Charles Lano	Chief Information Security Officer	June 23, 2021
Andy Wu	Chief Enterprise Architect	April 16, 2021
Theresa Giles	Chief, ITSD DCOSB Enterprise Services Section	June 23, 2021
Edwin Lieu	Information Technology Manager I	June 23, 2021
Richard Bannister	Systems Software Specialist III (Supervisor)	June 23, 2021

3. Purpose Statement:

This document's objective is to provide a cloud governance framework from which decisions, policies, and processes will emerge. With guidance from Microsoft's Cloud Adoption Framework for Azure governance model, this document will help to ensure that CDPH's Azure Cloud workloads, resources, and services as well as the platform on which they run comply with its established policies and regulatory obligations, thus providing a robust, secure, and cost-effective cloud-based data center.

4. Executive Summary

California Department of Public Health's (CDPH), Azure cloud environment was launched in 2017 in pursuit of agility and flexibility in meeting the demands of its customers, both internal and external.

With multiple business units engaging in the creation of resources and the consumption of IaaS, PaaS, and SaaS services, CDPH has expressed the following concerns:

- Azure users with owner or contributor roles can provision any resources without restrictions
- Administrative delegation has neither scoped boundaries nor expiration dates
- Resource hierarchy is flat and unsegmented
- Cost management and proactive cost containment are difficult
- Address HIPAA regulatory compliance requirements
- *"Who did what, when, and why?"* are difficult to ascertain
- Additional issues identified in the following Risk Assessment (next chapter)

This document provides a starting point to address these and other issues related to Azure governance. It provides an overview of the controls, services, and guidance provided by Microsoft to support the planning, architecture, acquisition, deployment, operation, and management of an Azure enterprise environment.

5. Risk Assessment with Solutions Through Governance

Any change to a business process or technology platform will always introduce risk. CDPH's extension of its on-premises data center in Rancho Cordova to Azure Cloud is no exception. With guidance from the Cloud Adoption Framework for Azure and its disciplines of cloud governance, we conducted a risk assessment during the period of January – March 2021. Here are the results:

IDENTIFIED RISK & ASSOCIATED CLOUD GOVERNANCE DISCIPLINE	HOW DOES THIS RISK AFFECT CDPH?	GOVERNANCE SOLUTION
Delegated privileges exceed intended administrative boundaries **[SECURITY BASELINE]**	A lack of resource segmentation results in administrative delegation that exceeds intended boundaries. **(HIGH RISK)**	Establish a well-designed segmentation strategy to contain risk and provide administrative delegation. See

IDENTIFIED RISK & ASSOCIATED CLOUD GOVERNANCE DISCIPLINE	HOW DOES THIS RISK AFFECT CDPH?	GOVERNANCE SOLUTION
		Chapter 8: Resource Hierarchy on page 15.
Granular permissions specifically reference individual user accounts. **[SECURITY BASELINE]**	Specific permissions based on individual user accounts create complexity and confusion as they do not carry the intended security posture into new or similar resources. This results in a complex security delegation structure that is difficult to maintain and change, thus negatively impacting both security and solution agility. **(HIGH RISK)**	Replace individual user accounts with Azure AD Groups for delegation. See ***Chapter 12: Role Based Access Control*** on page 78.
Access delegations persist cumulatively and indefinitely and are not subject to a regular audit process. **[SECURITY BASELINE]**	Without being subjected to a regular review, access delegations persist and accumulate over time violating the fundamental security principle of least privilege. **(HIGH RISK)**	To reduce the risk of stale access, CDPH can enforce a periodic audit and recertification of users' group memberships, access to enterprise applications, and role assignments. See ***Chapter 13: Identity Governance: Entitlement Management*** on page 100.
Mechanisms that support regulatory compliance are not in place. **[SECURITY BASELINE]**	Microsoft provides automation for HIPAA/HITRUST compliance in the form of blueprints, which are currently not in place. **(HIGH RISK)**	For existing environments, See ***Chapter 11: Policies*** on page 68. For new environments, see ***Chapter 16: Blueprints*** on page 126. For existing environments, deploy the individual policies in ***Chapter 19: What's Next? How Do We Move Forward from Here?*** on page 147. Other solutions include Azure Security Center and Splunk.

IDENTIFIED RISK & ASSOCIATED CLOUD GOVERNANCE DISCIPLINE	HOW DOES THIS RISK AFFECT CDPH?	GOVERNANCE SOLUTION
Users with appropriate privileges have no restrictions on the Azure resources and services they can create. **[SECURITY BASELINE]**	No control mechanisms in place preventing unauthorized actions with contributor privileges such as but not limited to: • Create a virtual machine with 24 CPUs and 488 GB of RAM for $10,276/month or deploy a Storage Account with potential PHI data without encryption • Create resources stored at a foreign or out of state location. **(HIGH RISK)**	Implement resource restrictions. See ***Chapter 11: Policies*** on page 68. Implement least privilege access. See ***Chapter 12: Role Based Access Control (RBAC)*** on page 78.
Shared Azure subscriptions translate into bewildering cost management due to a lack of visibility of individual program spending. **[COST MANAGEMENT]**	Without the ability to track real-time spending for each program, costs for Azure's "pay for what you use" model can very easily spiral out of control. **(HIGH RISK)**	Allocate unique subscriptions for each business unit program. Prevent unexpected spending by establishing budgets and alerting. See ***Chapter 15: Cost Management*** on page 117.
Critical Azure components are not protected from accidental deletion. **[SECURITY BASELINE]**	Users with owner or contributor roles can accidentally delete critical resources such as subscriptions, resource groups, or an individual resource which could lead to a catastrophic outage. **(HIGH RISK)**	Protect critical resources from inadvertent deletions through Resource Locks. See ***Chapter 14: Resource Locks*** on page 112.
Lack of an ongoing governance process that persists beyond this initial governance framework document. **[DEPLOYMENT ACCELERATION]**	While this document hopes to deliver an initial governance framework, CDPH will need to establish a governance process that empowers designated CDPH staff with 1) accountability; 2) authority; and 3) decision-making process. **(HIGH RISK)**	Develop a governance process with committed staff resources. See ***Phase 6: Develop a Process for Governance (Chapter 19: What's Next: How Do We Move Forward from Here?)*** on page 147.

IDENTIFIED RISK & ASSOCIATED CLOUD GOVERNANCE DISCIPLINE	HOW DOES THIS RISK AFFECT CDPH?	GOVERNANCE SOLUTION
Most of CDPH's Azure resources do not have logging enabled. **[SECURITY BASELINE]**	Resource logs provide critical insight into operations that performed within the Azure resource itself (in other words, data plane activities). Answers the fundamental questions of "Who? What? and When? cannot be ascertained without resource logs. **(HIGH RISK)**	Forward resource logs to Splunk through an Event Hub. See ***Logging and Retention Strategy for Azure Platform Log***s in ***Chapter 17: Monitoring for Compliance and Changes*** on page 133.
Log retention for Azure Activity Logs and Active Directory Logs are inadequate. **[SECURITY BASELNE]**	By default, Azure Activity Logs and Azure Active Directory Sign-in/Audit Logs are stored for 90 days and 30 days, respectively. These retention policies are generally insufficient for acquiring historical information for the purposes of security investigations, general troubleshooting, auditing access permissions, or facilitating da-to-day operations. Additionally, regulatory compliance requirements require a minimum of one year. **(HIGH RISK)**	Forward Activity Logs and Active Directory Logs to Splunk through an Event Hub. See ***Logging and Retention Strategy for Azure Platform Log***s in ***Chapter 17: Monitoring for Compliance and Changes*** on page 133.
Lack of operational foundational standards, procedures, and processes to ensure day-to-day operations of Azure cloud datacenter are well defined and delegated to staff with clear lines of responsibility.	Day-to-day operations such as backup strategies with established recovery time objectives (RTO) and recovery point objectives (RPO) have yet to be defined and documented. Note that backup strategies will change depending on the nature of the workload to be backed up. Baseline design and operations for common technologies have yet to be developed. Examples are:	While day-to-day operations procedures are out of scope for this document, another document called **"CDPH Azure Operations Guide for Baseline Components"** is currently under development.

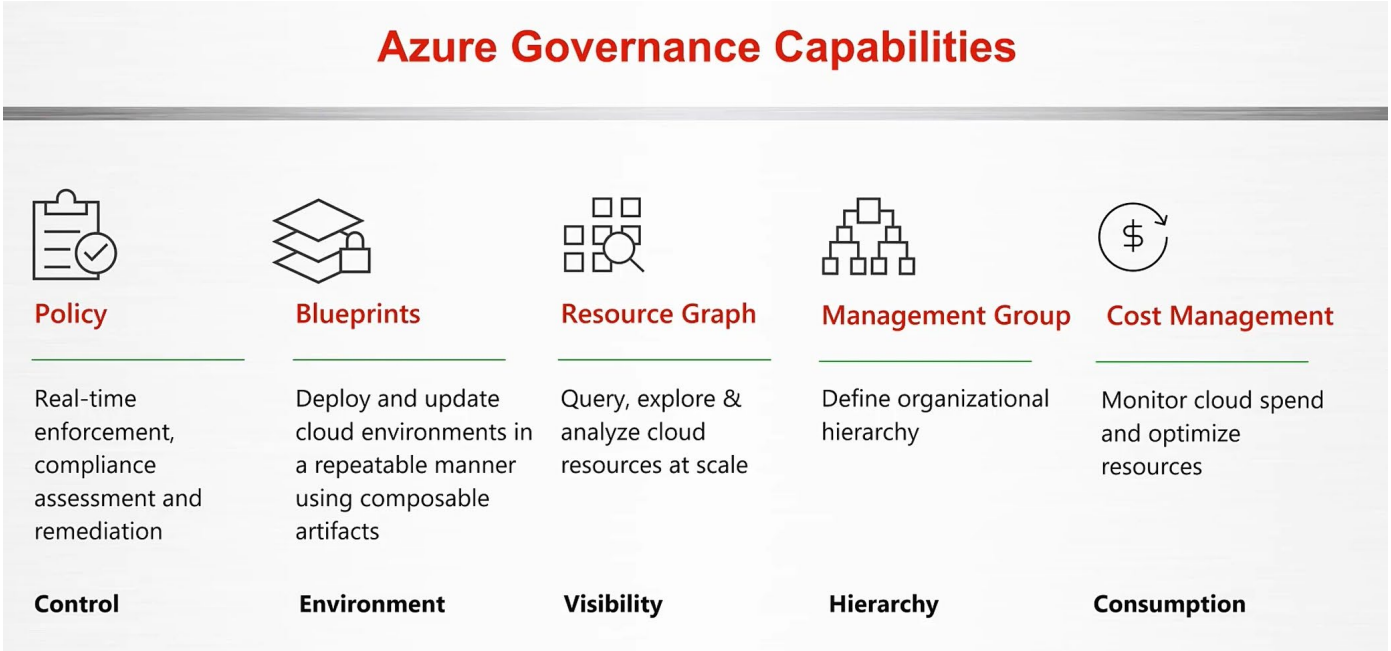
IDENTIFIED RISK & ASSOCIATED CLOUD GOVERNANCE DISCIPLINE	HOW DOES THIS RISK AFFECT CDPH?	GOVERNANCE SOLUTION
[DEPLOYMENT ACCELERATION]	• Azure Key Vault • Azure Storage • Azure SQL Server • Azure SQL Database • Log Analytics Workspace • Azure Load Balancer • Azure Application Gateway with WAF • Azure NSG • Azure Firewall **(MEDIUM RISK)** Currently Medium Risk. As cloud adoption grows, this will escalate into High Risk.	
No existing naming convention for Azure resources. **[RESOURCE CONSISTENCY]**	A consistent and well-defined naming convention facilitates the location of resources and provides an understanding of role, business unit owner, application workload, and environment at glance. It provides CDPH staff with clarity and consistency and facilitates collaboration across multiple business units and external vendors by establishing a standardized and logical naming pattern. **(MEDIUM RISK)**	Establish a consistent naming convention. See ***Chapter 9: Naming Conventions*** on page 27.
Who created a given Azure resource and when it was created is difficult to determine. **[IDENTITY BASELINE]**	Establishing ownership is key to CDPH's decentralized management environment. Knowing when a resource was created and by whom provides a foundation for effective response during an outage and simplifies collaboration across business units. **(MEDIUM RISK)**	Configure automatic tagging of user who created the resource and its date of creation. See ***Chapter 10: Resource Tags*** in page 63.
Leverage Entitlement Management to remove barriers to	Entitlement Management automates employee and partner access requests, approvals, auditing,	Deploy Entitlement Management. See ***Chapter 13: Identity Governance:***

IDENTIFIED RISK & ASSOCIATED CLOUD GOVERNANCE DISCIPLINE	HOW DOES THIS RISK AFFECT CDPH?	GOVERNANCE SOLUTION
internal and external collaboration and increase security. **[DEPLOYMENT ACCELERATION]**	and review. Entitlement Management provides administrators the ability to create, automate, and categorically group together necessary resources into what is called an access package with periodic access reviews to recertify continued access. **(MEDIUM RISK)**	***Entitlement Management*** on page 100.

6. Azure Tools for Governance

The focus of this document is cloud governance, and specifically, using Microsoft Azure as the cloud technology platform. Azure has grown rapidly since its introduction in 2008 and since governance is crucial to its success, Microsoft provides building blocks and tools that would aid in its deployment.

CDPH will utilize all governance capabilities that Azure provides, namely: 1) Policy, 2) Blueprints, 3) Resource Graph, 4) Management Group, and 5) Cost Management. This document will explore each of these capabilities in detail and propose ways to deploy them in the coming chapters.



7. Our Approach: Start Small with Minimal Viable Product (MVP)

Establishing cloud governance is a large iterative effort. Implementing a large-scale governance effort is a daunting strategy that could result in upper management push-back and unacceptable risk. Our approach embraces Microsoft's Minimum Viable Product (MVP) for governance which recommends we start small in order to establish a more realistic foundation from which CDPH can evolve and mature.

Our Minimum Viable Product (MVP) approach will deploy the least number of policies in the form of one HIPAA initiative, a naming convention, a resource hierarchy, and resource tags. As CDPH's governance process evolves and matures, it can expand and branch out from there.

8. Resource Hierarchy

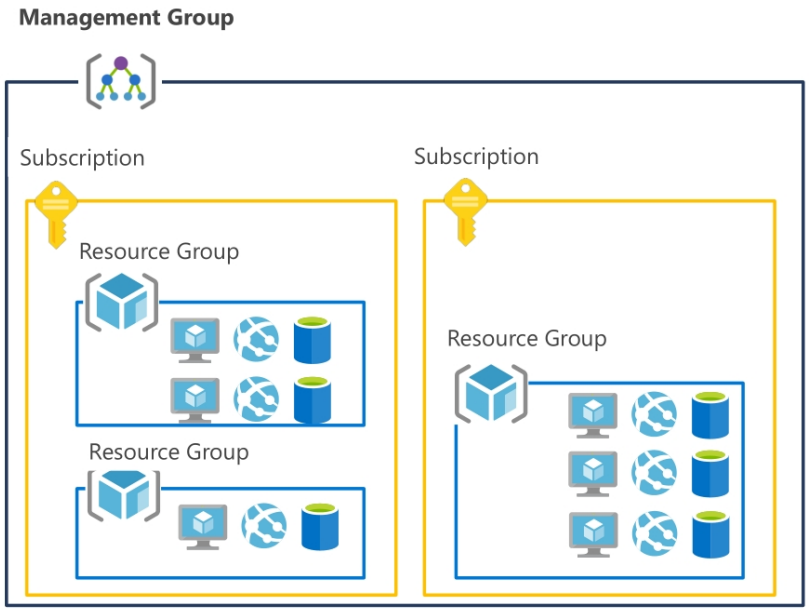
The first step in CDPH's journey to governance is establishing an organizational design for resources. An efficient Azure governance framework emanates from a well thought-out and executed resource hierarchy. It describes how Azure management groups, subscriptions, and resource groups (along with the resources they contain) interact in an enterprise environment. Similar in concept to an Active Directory Organizational Unit (OU) structure, a well-designed resource hierarchy will allow CDPH to deploy both global and targeted policies in addition to user role assignments in a manner which flow down the hierarchy (through inheritance) with minimal effort and maintenance.

Resource Organization in Azure

1. **Management groups**: To reflect security, operations and business/accounting hierarchies

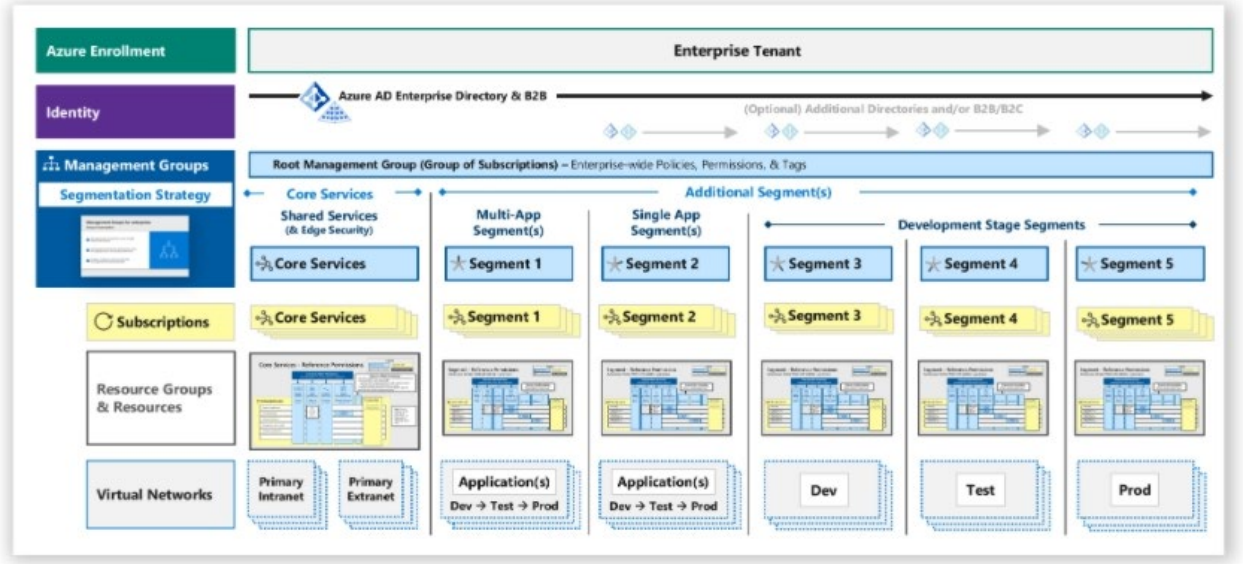
2. **Subscriptions**: To group resources for the same purposes into logical collections

3. **Resource groups**: To further group applications or workloads into deployment and operations units

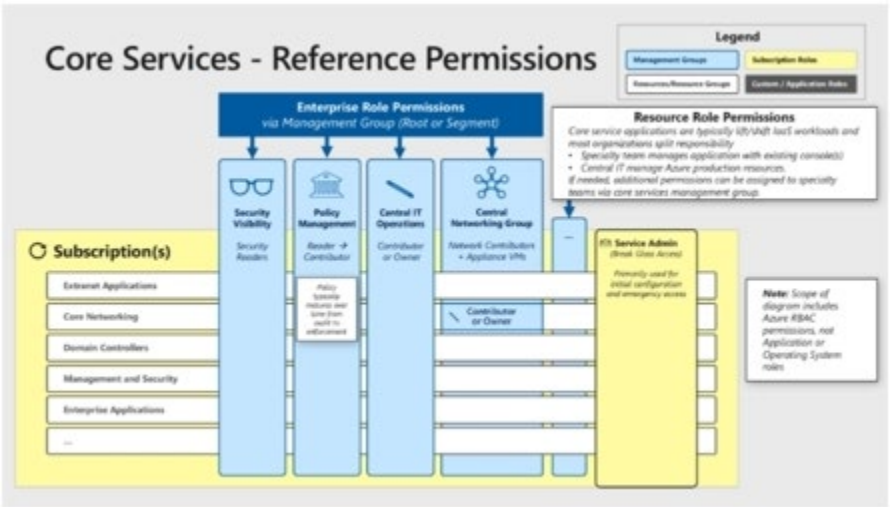


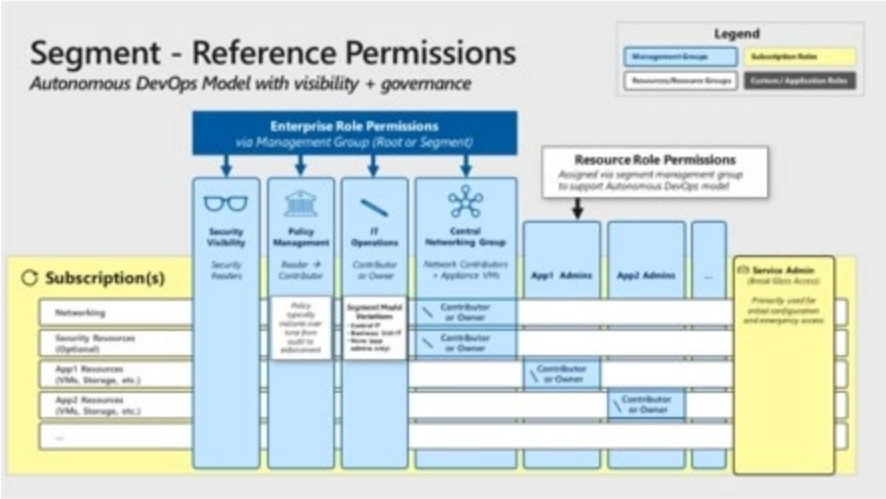
Segmentation Strategy Reference Model

According to Microsoft: "Segmentation refers to the isolation of resources from other parts of the organization. It's an effective way of detecting and containing adversary movements." This prescriptive guidance is encapsulated by the following reference model diagram (below).



SOURCE: Reference model for enterprise segmentation. [Segmentation strategies - Azure Architecture Center | Microsoft Docs]





SOURCE: Security Management Groups [Security management groups - Azure Architecture Center | Microsoft Docs]

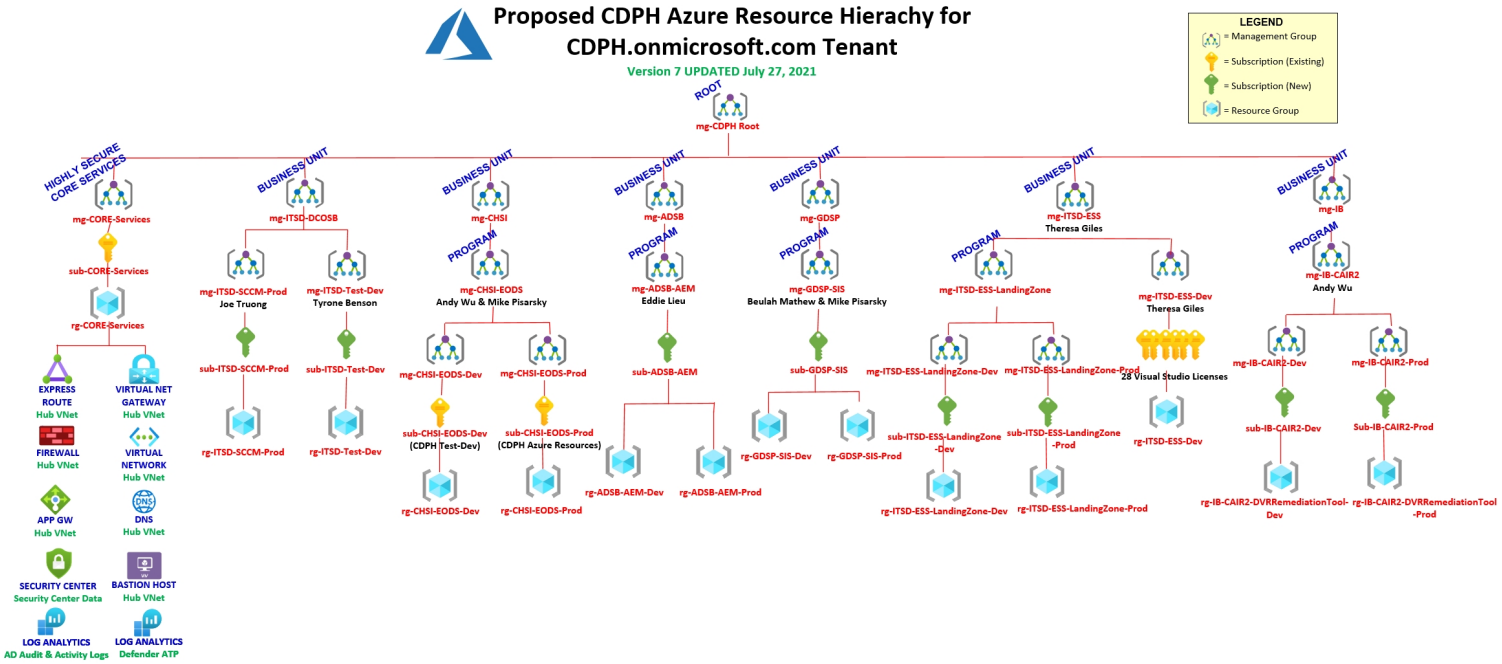
From the preceding segmentation reference models, our take-aways are as follows:

- Segmentation strategy is based on management groups. Microsoft recommends no more than two levels (excluding root management group).
- Establish a management group for core services that are utilized across the entire organization. This will allow CDPH to isolate sensitive and critical workloads from compromise by other assets.
- Use management groups for each workload segment represented by teams with limited scope of responsibility due to organizational boundaries.
- Root Management Group will serve as the repository for all custom CDPH policies, initiatives, and blueprint artifacts.
- Resource groups should be deployed in a manner that are developed together, managed together, and retired together belong in the same resource group.

The resource hierarchy below is based on CDPH's business units and their programs. This approach would allow CDPH to target administrative delegation precisely at the business unit level thus empowering business unit managers the ability to in turn manage their own resources and provide access to these resources to staff. Additionally, subscriptions will be associated with each business unit thereby providing business unit managers the ability to efficiently keep track of costs and utilization.

Deploying business unit program management groups at the third level would provide business unit managers the ability to manage their programs' individual environments (development, staging, and production) and through the use of Resource Groups for each of these environments to further delegate access to these resources with increased granularity (i.e. staff working on Dev will not have access to Production). Segmentation at this level would serve to further isolate publicly accessible systems in production from being used by an attacker as a pivot to other systems.

The resource hierarchy is shown below:



Benefits of Resource Hierarchy

- Delegation of least use privileges through organizational boundaries and program boundaries.
- Minimize operational friction by aligning the hierarchy each business unit's program boundaries.
- Isolation of workloads by compromise through other assets.
- Provide oversight to prevent sprawl and unintended costs
- Assigns a subscription for each business unit and the programs they manage which serves as a foundation for effective cost management.

Subscription Planning

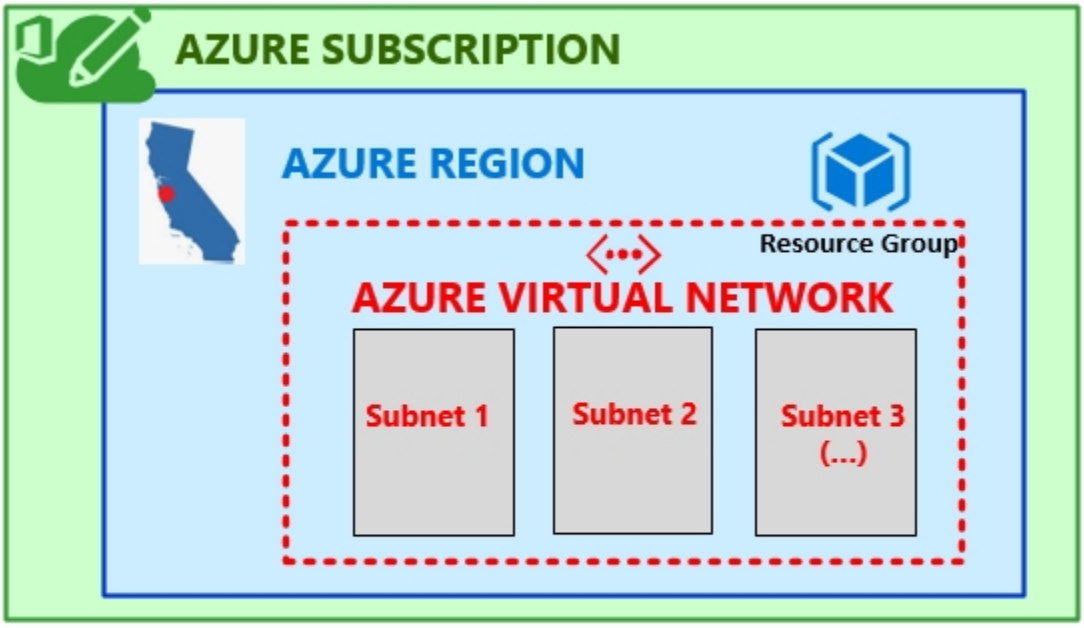
Effective subscription design helps organizations establish a structure to organize and manage assets in Azure. Each resource in Azure, such as a Databricks Service, or a Storage Account is associated with a subscription. The resource hierarchy illustrated in the previous section necessitates the allocation of a separate subscription for each business unit and the programs they manage. Microsoft's best practice recommendation is to further segregate environment workloads by subscriptions as well: one subscription for development and testing and another for production.

As in the case of CHSI's EODS Program, several individual projects can emerge from a program and the business unit may opt to deploy these various projects from within the same subscription.

Hub and Scope Network Design

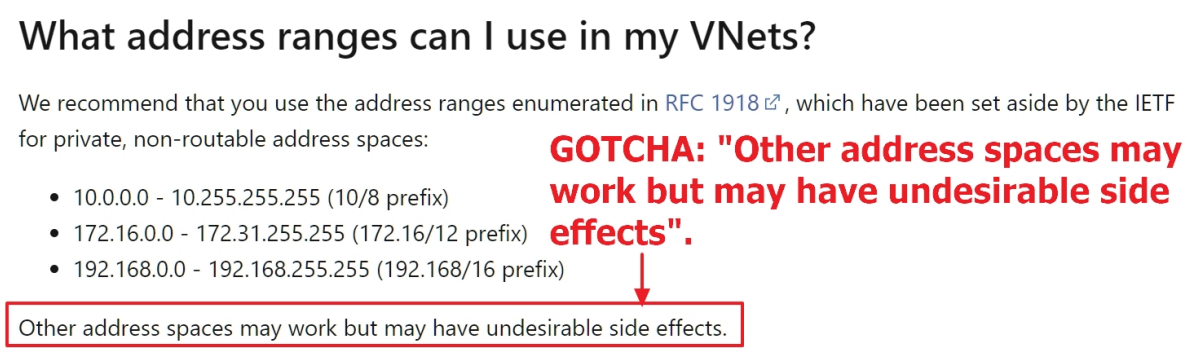
The following network design incorporates the previously discussed elements of the resource hierarchy including subscriptions and resource groups and incorporates CDPH's existing n-tier architecture-based design principles. The result is a hub and spoke architecture with the following design components:

- Virtual Networks (VNets) is a logical isolation of the Azure cloud dedicated to each subscription. VNets can be further segmented into subnets. By default, all resources within the same VNet can communicate with each other, even across subnets. Network Security Groups allow restricting inbound and outbound traffic flow to individual subnets.
- The hub (upper left corner of the diagram) contains core shared services such as (but not limited to) the VPN gateway (ExpressRoute), firewall, bastion host, application gateway, and DNS.
- The spokes represent a virtual network associated with a resource group (Development, Staging, or Prod) that is contained within a subscription (CHSI-EODS-Dev-01).
- For a VNet to communicate with another VNet, a peering relationship will need to be established.
- For a spoke virtual network to gain connectivity to CDPH resources outside of the virtual network, or to the internet, it will need to traverse the hub.
- Subscriptions are an integral component of Azure network design as virtual networks (VNets) cannot span across subscriptions. The diagram shows one hub VNet and four spoke VNets. Each of these four virtual networks exist within their own unique subscription.



FUNDAMENTAL CONCEPT: A VNet is contained within a Resource Group which is contained within a Region which is associated with a Subscription. Thus, VNets cannot span Subscriptions.

- The hub network contains an application gateway (HTTPS only to spoke networks)) and firewall (all traffic except HTTPS to spoke networks) deployed in parallel.
- The diagram shows a hub firewall connecting to spoke application gateways. While deploying an application gateway in this manner adds very little value as an upstream firewall cannot decrypt and inspect the traffic, this is the way application gateways are currently deployed at CDPH on prem. The F5 application gateway sits behind the ASA firewall to provide CDPH with the ability to control all traffic flow through the firewall.
- Each virtual network can have multiple subnets that hosts a specific tier (Web, Application, Data).
- Each subnet will be locked down by a Network Security Group which contains rules that allow or deny inbound or outbound traffic.
- A load balancer sits upstream of SQL Server DB1 and DB2 to load-balance workload.
- For 99.99% availability, Azure Availability Zones are demonstrated in the diagram. Each web server (VM1, VM2, and VM3) and SQL database are housed in separate Availability Zones (physical datacenters within an Azure region).
- Addresses spaces used cannot overlap with the 10.0.0.0/8 IP address space already allocated with CDPH's on-premises resources. The IP addresses spaces allow for easy identification of hub VNets (192.168.0.0/16) and spoke VNets carved out of 172.16.0.0/12 address space based on requirements of a given program. For instance, some programs will only require four IP addresses while others could require 30.



REFERENCE: [Azure Virtual Network FAQ | Microsoft Docs]

- Expanding a given VNet's IP address space will require the VNet peering relationship to be deleted then recreated. It is always best practice to provide adequate IP addresses and allow for growth instead of having to expand an IP address space.

Things to Remember When Viewing Hub and Spoke Network Diagram:

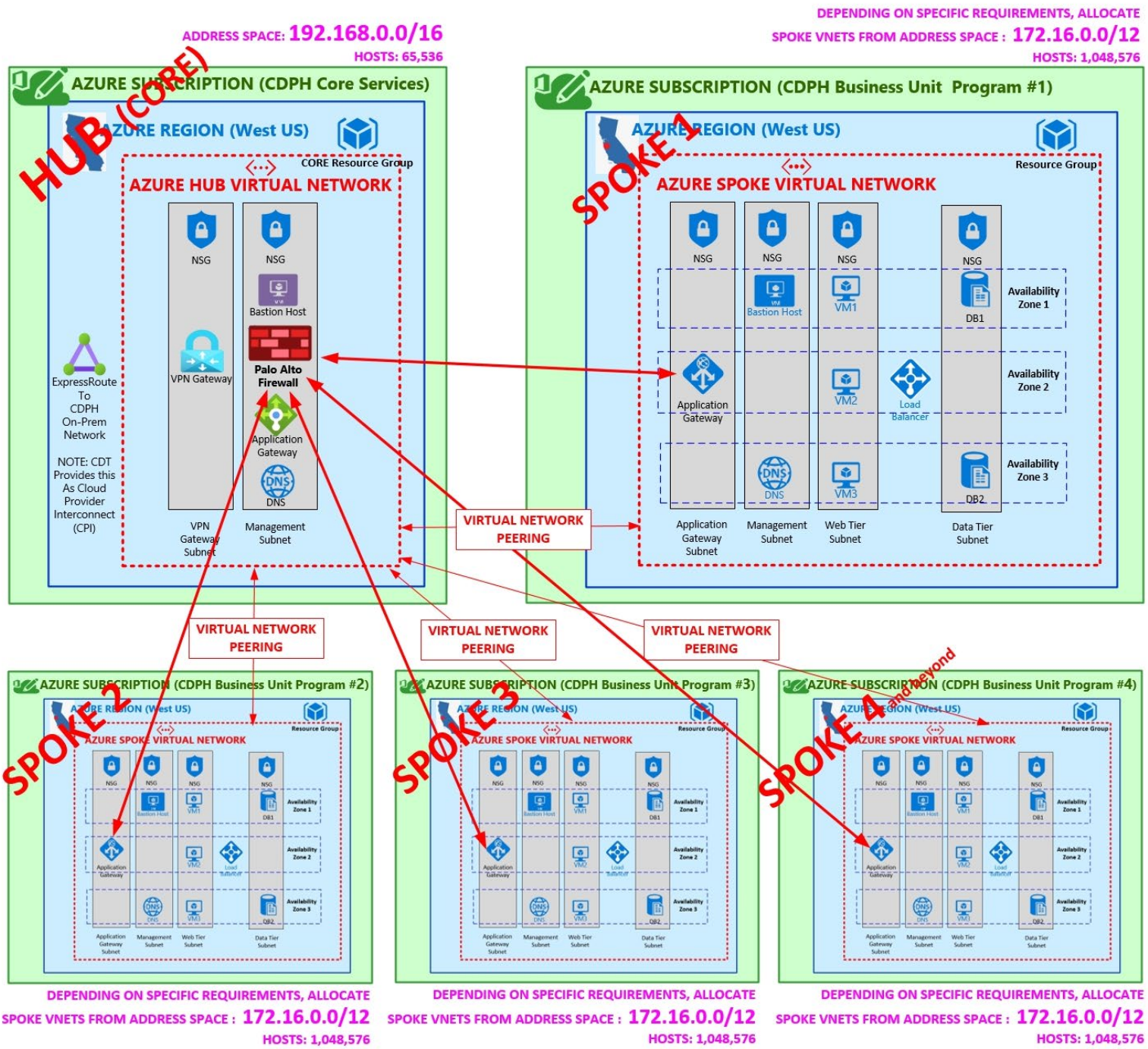
1) The diagram shows one hub and four spokes. The actual implementation can have as many spoke VNets as required. Azure has a limit of 1,000 VNets per region per subscription.

2) Spokes 2, 3, and 4 have been shrunk to fit the page.

3) Spoke elements are for demonstration only. Each business unit program may or may not utilize all elements shown or may choose to deploy different elements such as Web Apps instead of virtual machines.

4) Spoke Application Gateways (layer 7 load balancer with built-in Web Application Firewall) sit behind hub firewall at core network. Application Gateway deployed side-by-side is recommended design as Azure firewalls cannot decrypt HPPTS traffic. Alternately, hub Application Gateway may be used to connect to spoke resources.

PROPOSED CDPH HUB AND SPOKE NETWORK DESIGN



Spoke Network Address Space Allocation Planning

Virtual network address space planning is a critical step as address spaces can never overlap. With CDPH's on-premises network address space already allocated to 10.0.0.0 /8, and with the above-mentioned hub network allocated to 192.168.0.0 /16, spoke network address space planning will require the use of the following table in the next page.

GOTCHA: Extending an existing address space requires an existing network peering relationship to be deleted and recreated, which necessitates an outage window. Through proper planning, it is best to avoid extending an address space whenever possible.

GOTCHA: Avoid using static IP address assignments unless absolutely required as it may break at some point. Let Azure DHCP and Azure DNS handle dynamic IP address allocation and registration, respectively.

OPERATIONS BEST PRACTICE: Ensure that the role of allocating address spaces to VNets is assigned to only one primary staff member (with backup staff taking over during primary staff member's absence). An authoritative source of address space allocation helps avoid problems with overlap. Consider using Infoblox DDI for Microsoft Azure for IP address management (IPAM, levering existing staff skillset in on-prem Infoblox DHCP, DNS, and IPAM.

Spoke Network Address Space	Spoke Subnet Mask	Maximum Subnets	Total IPs per Subnet	Azure Usable IPs per Subnet See Gotcha Below
172.16.0.0 / 12	255.240.0.0	16	1,048,576	1,048,571
172.16.0.0 / 13	255.248.0.0	32	524,828	524,823
172.16.0.0 / 14	255.252.0.0	64	262,144	262,139
172.16.0.0 / 15	255.240.0.0	128	131,072	131,067
172.16.0.0 / 16	255.255.0.0	256	65,536	65,531
172.16.0.0 / 17	255.255.128.0	512	32,768	32,763
172.16.0.0 / 18	255.255.192.0	1,024	16,384	16,379
172.16.0.0 / 19	255.255.224.0	2,048	8,192	8,187
172.16.0.0 / 20	255.255.240.0	4,096	4,096	4,091
172.16.0.0 / 21	255.255.248.0	8,192	2,048	2,043
172.16.0.0 / 22	255.255.252.0	16,384	1,024	1,019
172.16.0.0 / 23	255.255.254.0	32,768	512	507
172.16.0.0 / 24	255.255.255.0	65,536	256	251
172.16.0.0 / 25	255.255.255.128	13,072	128	123
172.16.0.0 / 26	255.255.255.192	262,144	64	59
172.16.0.0 / 27	255.255.255.224	524,288	32	27
172.16.0.0 / 28	255.255.255.240	1,048,576	16	11
172.16.0.0 / 29	255.255.255.248	2,097,152	8	3

LEGEND:

= Microsoft best practice is to avoid using these due to potential for excessive waste.
= CDPH will likely use these address spaces for most programs/projects (sweet spot).

GOTCHA: Each subnet loses 5 IP addresses as shown here:

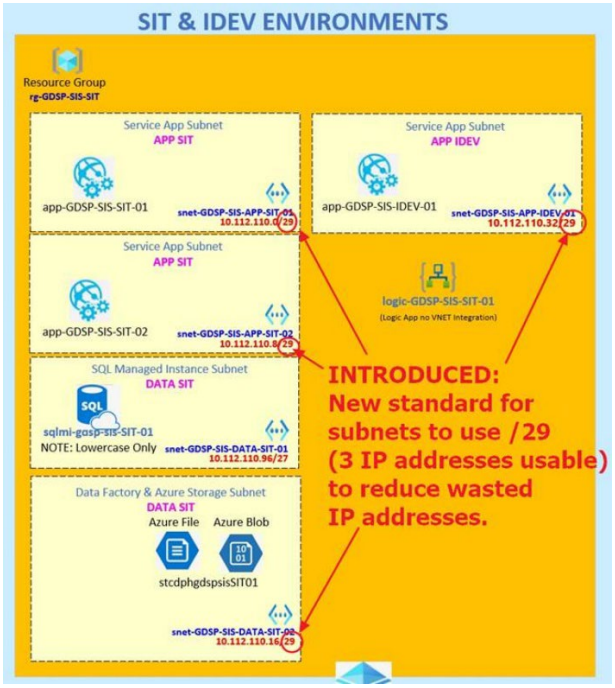
- x.x.x.0 is reserved as the Network address as per RFC 1812.
- x.x.x.1 is **reserved by Azure** as the Default Gateway.
- x.x.x.2 – x.x.x.3 is **reserved by Azure** to map the Azure DNS IPs to the VNet space.
- x.x.x.255 is reserved as the Network broadcast address as per RFC 919.

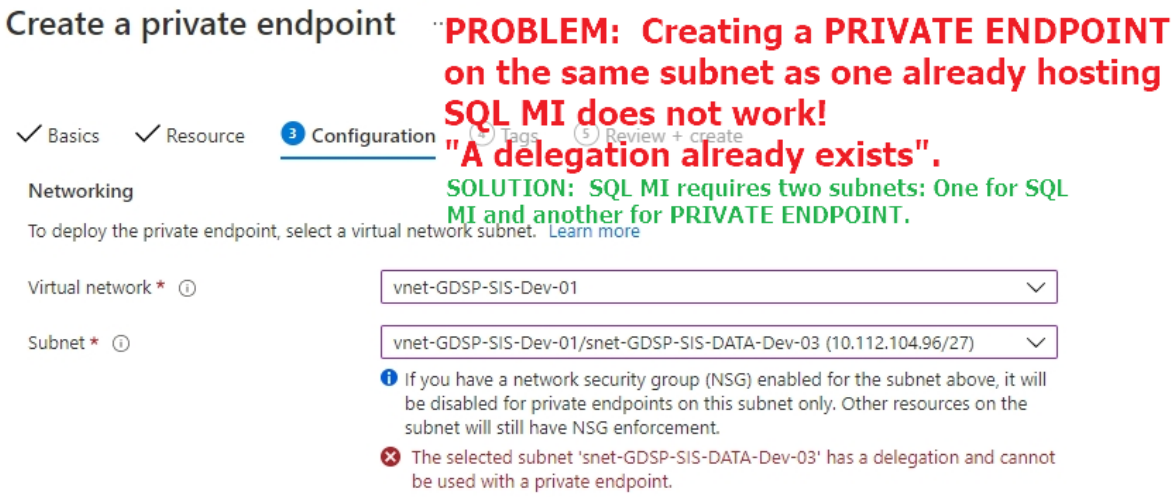
REFERENCE: Azure Virtual Network FAQ | Microsoft Docs

GOTCHA: Microsoft recommends **/27 (255.255.255.224)** as the bare minimum CIDR prefix. In other words, deploying a subnet smaller than **/27** is not recommended.

DECEMBER 15, 2021 UPDATE: Address Space Allocation Strategy for Subnets to use /29 mask.

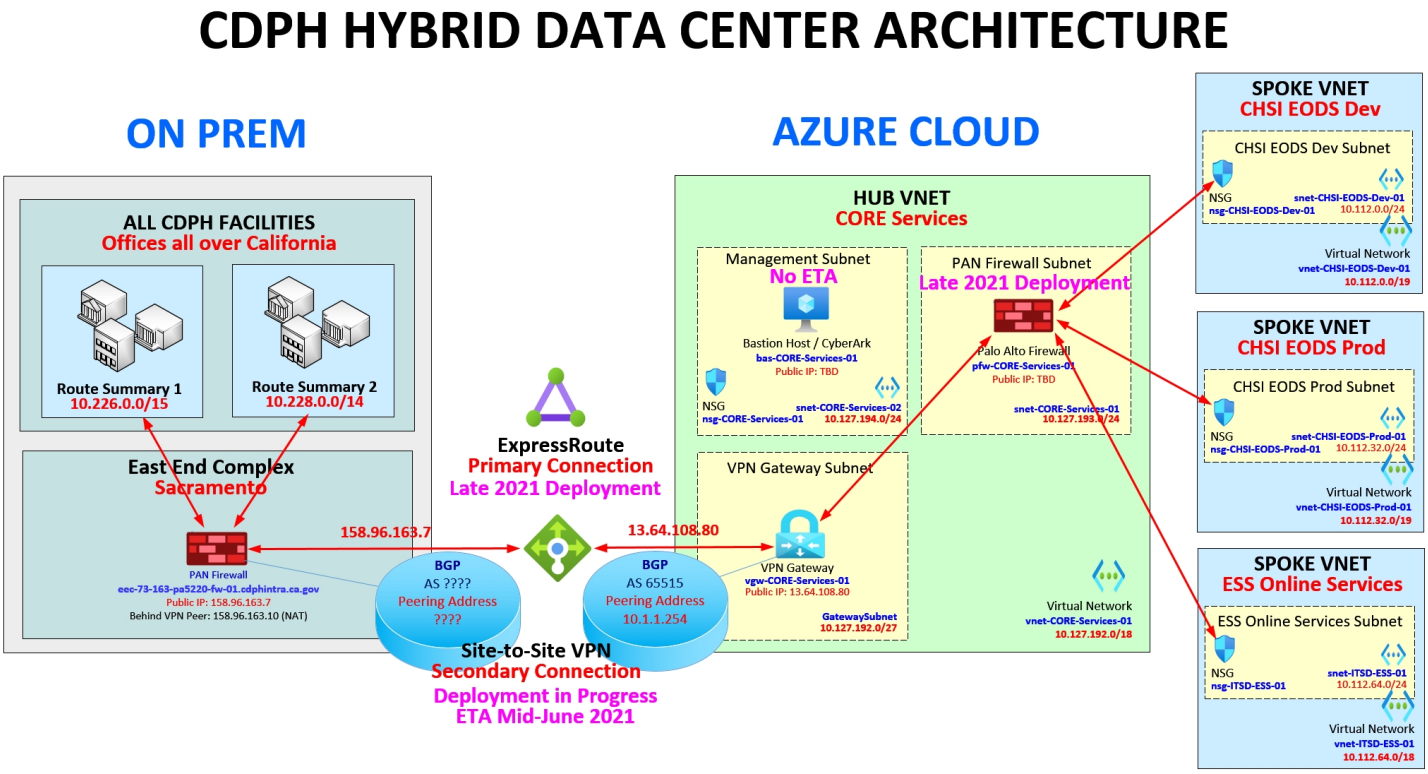
The new standard of deploying /29 subnets which yield three useable IP addresses (the smallest subnet supported by Microsoft) addresses the concern of wasting IP addresses whenever common Azure resources such as SQL MI and App Services are deployed, which require delegation to the entire subnet. In other words, once we deploy these resources, no other resources can share the same subnet. Standardizing on /29 will minimize unused IP addresses.





MAY 5, 2021 UPDATE: Address Space Allocation Strategy Provided by Richard Cabutage on 2021-5-24

The diagram below reflects Richard's recommendation of allocating 10.112.0.0/12 for all Azure cloud resources and using a /18 address space for all VNets across the board. This provides each program/project the ability to create a maximum of 1,024 subnets with 16,382 host per subnet. Currently, we have two programs/projects: EODS Databricks and ESS Online Services. The initial /18 allocation for EODS Databricks is shown further subdivided into /19 between their Dev and Test environments. IN SUMMARY: A /18 allocation provides maximum flexibility while minimizing administrative overhead.

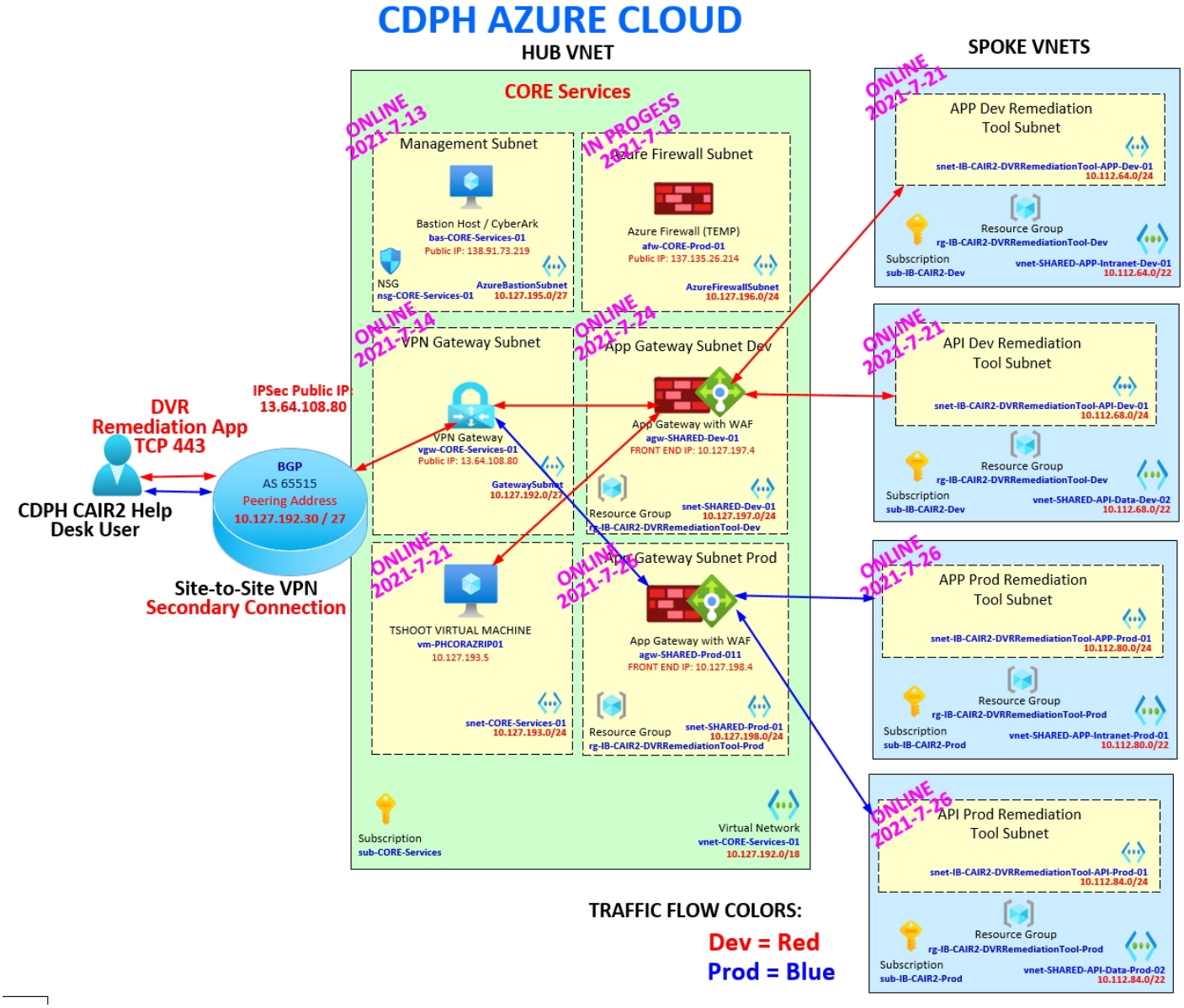


Additional Notes:

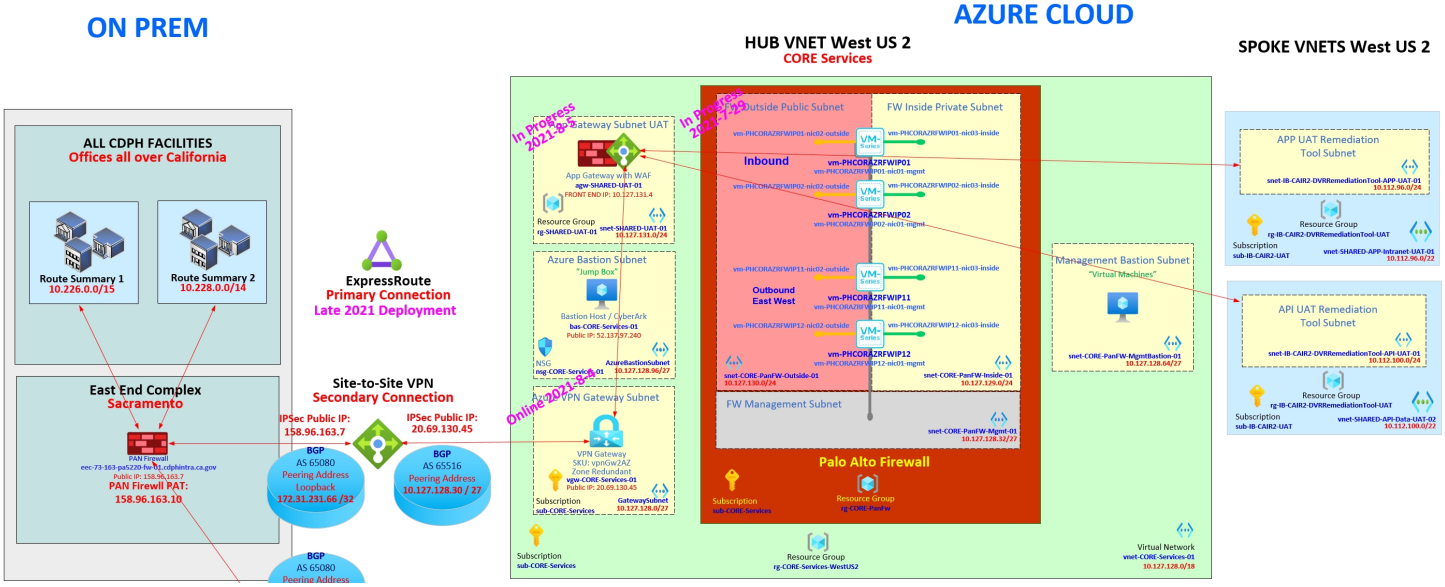
- Absent the PAN Firewall, we will use Network Security Groups (NSG) which provide very basic firewall functionality in the interim.
- Once the PAN comes online, NSGs will complement it by providing full isolation at the subnet level.
- Site-to-Site VPN becomes the secondary connection once ExpressRoute comes online.

JULY 28, 2021 UPDATE: Immunization Branch's CAIR2 Digital Vaccine Record (DVR) Project Deployment Completed as of July 28, 2021:

CAIR2 DVR ARCHITECTURE



AUGUST 11, 2021 UPDATE: The Palo Alto Firewall (large red box below) is about to go live next week. Here is the architectural diagram as it relates to App Gateway and the Spoke VNets.



9. Information Security Office PAM Security Standard (This section written and maintained by the ISO's Cannic Hung)

1. All user IDs on CDPH Azure AD tenant must be constructed according to the CDPH user ID naming convention, and must conform the following:

Azure Privileged User ID:

- [First Name].[Last Name]_A@cdph.ca.gov

Azure Privileged Legacy User ID:

- [First Name Initial].[Last Name]@cdph.onmicrosoft.com

Azure Non-Privileged User ID:

- [First Name].[Last Name]@cdph.ca.gov

In a scenario where duplicate first and last names existed, CDPH must add a numeric suffix starting at 2 and increment it by 1 for each subsequence duplicate name.

1. All privileged non-human IDs on CDPH Azure AD tenant must be constructed according to the CDPH naming convention, and must conform the following:

   Azure User-Assigned Managed Identity Name:

   - **mid-[Owner]-[App]-[Env]** where:
     - **mid**: Prefix for all user-assigned managed identity
     - **Owner**: Program area of the privileged non-human account
     - **App**: Application name
     - **Env**: Environment - dev = development; test = testing; stag = Staging; prod = Production
   - The length limitation of the name parameter is 24 characters
   - Allowable characters are (0-9, a-z, and A-Z) and the hyphen (-)

2. In CDPH Azure AD tenant, Azure Access Reviews must be used to manage inactive privileged user accounts, inactive guest user accounts, group, and role memberships. Multiple Group Owners (at least two) must be defined when creating an Azure AD Group. Group Owners are expected to be used as the designated reviewers when creating an Azure Access Reviews.

2. Naming Conventions

"The beginning of wisdom is the ability to call things by their proper names." -- Confucius

A well-chosen name helps CDPH quickly identify the Azure resource's type, its associated business unit owner, its business unit program or application, its deployment environment, and finally, its instance.

NAMING CONVENTION OBJECTIVES:

- Facilitate the location of resources and understand their role, business unit owner, application workload, and environment at glance. Strive for clarity and consistency.
- Facilitate collaboration across multiple business units and external vendors by establishing a standardized and logical naming pattern.

- When viewed from the Azure portal, all related Azure resources should appear in proximity to each other when viewing a list of Azure resources.
- In the event of a security incident, CDPH needs to be able to quickly identify affected systems, which business unit owns them, what functions they support, their level of criticality, and the overall business impact. Azure security services such as Security Center references resources by name. It is critical to be able to read logs and alert with resources that are named descriptively.
- Facilitate automation through Azure Resource Management (ARM) templates, PowerShell, Power CLI, other mechanisms.

Mandatory Naming Convention Rules in Azure

Before CDPH establishes its naming conventions, it helps to first understand what is not allowed in Azure. Note that some Azure entities such as Storage Account Names, have restrictions such as lowercase only and no hyphens.

Azure Entity	Length	Casing	Valid Characters
Resource Group	1–90	Case insensitive	Alphanumeric, underscore, parentheses, hyphen, period (except at end), and Unicode characters that match the regex.
Tag	512 (name), 256 (value)	Case insensitive	Alphanumeric
Virtual Machine	1–15 (Windows), 1–64 (Linux)	Case insensitive	Alphanumeric and hyphen
Storage account name (disk)	3–24	Lowercase	Alphanumeric
Virtual Network (VNet)	2–64	Case insensitive	Alphanumeric, hyphen, underscore, and period
Subnet	2–80	Case insensitive	Alphanumeric, hyphen, underscore, and period
Network Interface	1–80	Case insensitive	Alphanumeric, hyphen, underscore, and period
Network Security Group	1–80	Case insensitive	Alphanumeric, hyphen, underscore, and period

CDPH Note: Pay attention to these restrictions in particular.

NAMING CONVENTION: Management Groups

The management group name has two parts: 1) an ID and 2) Display Name. The unique ID cannot be changed once established and will be used henceforth mainly for automation purposes. The Display Name is user-friendly and can contain spaces.

HOW WE USE UPPER CASE: We use UPPER CASE to denote ownership. In the examples that follow, which just happens to use CHSI (the business unit with the

most Azure resources at the time of this writing), a resource with UPPER CASE "CHSI EODS" means it is owned by the EODS program of the CHSI business unit.

Level 1: Root Management Group

Name: mg-CDPH-Root
ID: 1f311b51-f6d9-4153-9bac-55e0ef9641b8
(cannot change)

Level 2: Business Unit Management Group

Name: mg-CHSI
ID: mg-CHSI
Resource Type | Business Unit

Level 3: Business Unit Program Management Group

Name: mg-CHSI-EODS
ID: mg-CHSI-EODS
Resource Type | Business Unit | Business Unit Program

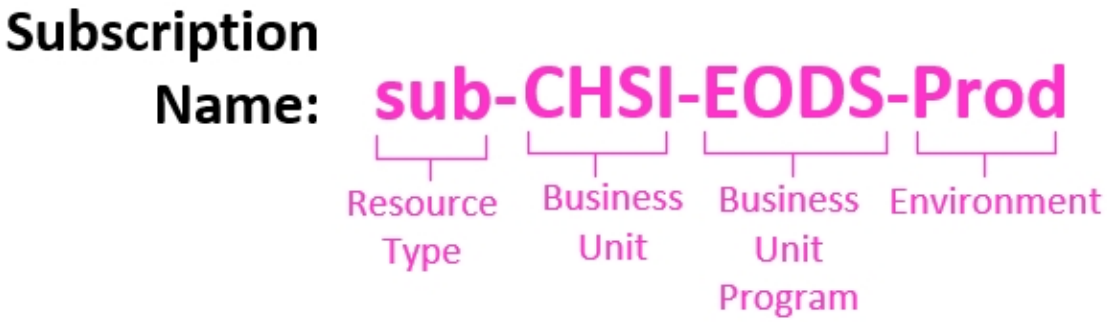
Naming Component	Description
Resource Type	The type of Azure Resource or Service. Examples: • Management Group -(mg) • Resource Group – (rg) • Storage Account – (sa) • Databricks Service – (dbs) REFERENCE:

	Recommended abbreviations for Azure resource types - Cloud Adoption Framework | Microsoft Docs
CDPH Business Unit	The business unit which owns the management group
CDPH Business Unit Program	The specific program, application, or workload associated with the subscription.
Environment	• Development (Dev) • Staging (Stag) • Production (Prod)

NAMING CONVENTION: Subscriptions

All Azure subscriptions' names have two components: 1) A unique ID and 2) a friendly name. The unique ID is assigned by Azure and cannot be changed. A recommended practice is to rename the friendly name to a standard that is appropriate to the environment.

The advantage to the subscription naming convention below is that the name matches the resource hierarchy to which it is associated. In other words, by looking at the name, you know which business unit and program management group the subscription belongs.

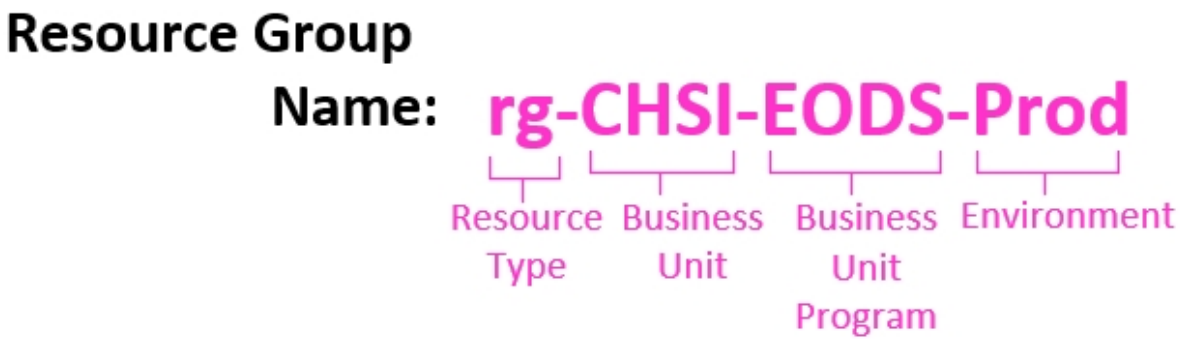


Naming Component	Description
CDPH Business Unit	The business unit who owns the subscription.
CDPH Business Unit Program	The specific program, application, or workload associated with the subscription.
Environment	• (Dev) - Development • (Stag) - Staging • (Prod) - Production

NAMING CONVENTION: Resource Groups

In Azure, Resource Groups are used to manage all resources that make up a solution (in this case, a Business Unit Program). From an Azure Governance perspective, CDPH has Management Groups that contain one or more subscriptions, with each subscription containing one or more Resource Groups. Resource Groups are also used in scoping Policies or Initiatives.

GOTCHA: As with a lot of Azure entities, Resource Groups cannot be renamed (as of March 2021). Resources will need to be moved to a new Resource Group bearing the desired name. Dependencies such as role assignments and scripts will require recreation and updates to new resourceIDs, respectively.



Naming Component	Description
Resource Type	The type of Azure Resource or Service. The only option is (rg) - Resource Group
CDPH Business Unit	The business unit who owns the management group.
CDPH Business Unit Program	The specific program, application, or workload associated with the subscription.
Environment	• (Dev) - Development • (Stag) - Staging • (Prod) - Production

NAMING CONVENTION: RBAC Groups for Security Delegation

Role-based access control (RBAC) is a component of the governance framework for organizations. RBAC ensures that only authorized and approved users have appropriate access to resources. In Azure, RBAC has over 120 built-in predefined roles that you can use to grant access at the management group, subscription, resource group, or resource level.

Azure Active Directory Group Name: rbac-GDSP-SIS-Prod-ea-PowerPlatform-GlobalAdmin-Custom

Naming Component	Description
Prefix	All RBAC Azure AD Groups will have a prefix of (rbac)
RBAC Scope Location in Resource Hierarchy	The name of the location in the resource hierarchy in which RBAC permissions are granted. The RBAC Scope Location is made up of three components: CDPH Business Unit: The business unit who owns the management group. CDPH Business Unit Program: The specific program, application, or workload associated with the subscription. Environment: (Dev) - Development; (Stag) – Staging; (Prod) - Production
RBAC Scope Type	The type of scope in which the RBAC role assignment will take place: • (mg) Management Group – whenever possible CDPH will scope RBAC assignments at this level. • (rg) Resource Group – scope RBAC at this level when only when a more granular delegation needs to be made. • (ea) Enterprise Applications - Enterprise Applications • (cat) Catalog – scope RBAC for Entitlement Management Access Package Catalogs.

	• (ir) Individual Resource – only on certain exceptions, scope RBAC at the resource level. Use the resource abbreviation for the specific resource: (sa) – storage account. Recommended abbreviations for Azure resource types - Cloud Adoption Framework | Microsoft Docs
(OPTIONAL) For **Enterprise Applications** Only	Azure hosts more than 3,600 third-party (and some by Microsoft) Enterprise Applications and growing. These applications are pre-federated and ready for use with Azure AD as the federation broker. The use of Azure AD RBAC groups are different for enterprise apps as they are for management groups and resource groups in that the RBAC group is used ***from within the application*** to delegate certain administrative roles to members of the group. The example above shows Power Platform, which is an Enterprise App used by GDSP SIS.
RBAC Role Name	The name of the built-in RBAC role or custom role assignment. Examples listed below: • (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. • (StorageBlobDataContributor) - Read, write, and delete Azure Storage containers and blobs. • (LogAnalyticsContributor) – Can read all monitoring data and edit monitoring settings.
(OPTIONAL) Custom RBAC (should rarely be used)	In rare situations when built in RBAC roles do not meet the requirements, create a custom role, and flag the Azure AD group with (custom) at the end.

	Custom RBAC roles might possibly generate more risk and validation work since a custom role that works today may not continue to work six months from now in the dynamic world of Azure.

Helpful examples:

Description	Example
Contributor Role delegated to the Management Group for the IB CAIR2 DCVR Dev environment.	rbac-IB-CAIR2-DCVR-Dev-**mg**-CDPH-ContributorNoNetwork-CustomRole **See Appendix A for more information on this role.**
Contributor role delegated to the Resource Group of GDSP SIS' UAT environment.	rbac-GDSP-SIS-UAT-**rg**-CDPH- ContributorNoNetwork-CustomRole **See Appendix A for more information on this role.**
App Insights Contributor role delegated to the Resource Group for GDSP SIS' Staging environment.	rbac-GDSP-SIS-Stg-**rg**-AppInsightsComponentContributor
Users of GDSP SIS Dev's DP application (generates PDF files).	rbac-GDSP-SIS-Dev-**ea**-DP-Users
Administrators of IB CAIR2 DVR Remediation's Prod Enterprise Application.	rbac-IB-CAIR2-DVRRemediation-Prod-**ea**-Admins
All Users of the PrinterLogic Application. (NOTE: This is the equivalent of CDPHINTRA\Domain Users as it is a Dynamic Group)	rbac-CORE-**ea**-PrinterLogic-AllUsers
Log Analytics Reader for Sentinel in CORE services.	rbac-CORE-Services-**Sentinel**-LogAnalyticsReader

Description	Azure AD RBAC Group Assigned at Management Group
Root RBAC assignment at the Root management group	rbac-CDPH-Root-**mg**-Owner
LogAnalyticsContributor RBAC role assignment at the CHSI-EODS management group	rbac-CHSI-EODS-**mg**-LogAnalyticsContributor
Contributor RBAC role assignment at the CHSI-EODS management group	rbac-CHSI-EODS-**mg**-CDPH-ContributorNoNetwork-CustomRole **See Appendix A for more information on this role.**
Description	**Azure AD RBAC Group Assigned at Resource Group**
Owner RBAC role assignment at the CHSI-EODS-Dev resource group.	rbac-CHSI-EODS-Dev-**rg**-Owner
StorageBlobDataContributor RBAC role assignment at the CHSI-EODS-Dev resource group.	rbac-CHSI-EODS-Dev-**rg**-StorageBlobDataContribor
LogAnalyticsContributor RBAC role assignment at the ADSB-AEM resource group.	rbac-ADSB-AEM-**rg**-LogAnalyticsAnalyticsContributor
Description	**Azure AD RBAC Group Used with Enterprise Applications**
This Azure AD group will be used to provide Global Admin privileges from within the Microsoft 365 (Dynamics) application.	rbac-GDSP-SIS-Dev-**ea**-PowerPlatform-GlobalAdmin

This Azure AD group will be used to provide System Administrator privileges from within the Power Platform (Dynamics) application.	rbac-GDSP-SIS-Dev-**ea**-PowerPlatform-SystemAdmin
This Azure AD group will be used to provide System Customizer privileges from within the Power Platform (Dynamics) application.	rbac-GDSP-SIS-Dev-**ea**-PowerPlatform-SystemCustomizer
This Azure AD group will be used to provide Environment Maker privileges from within the Power Platform (Dynamics) application.	rbac-GDSP-SIS-Dev-**ea**-PowerPlatform-EnvironmentMaker

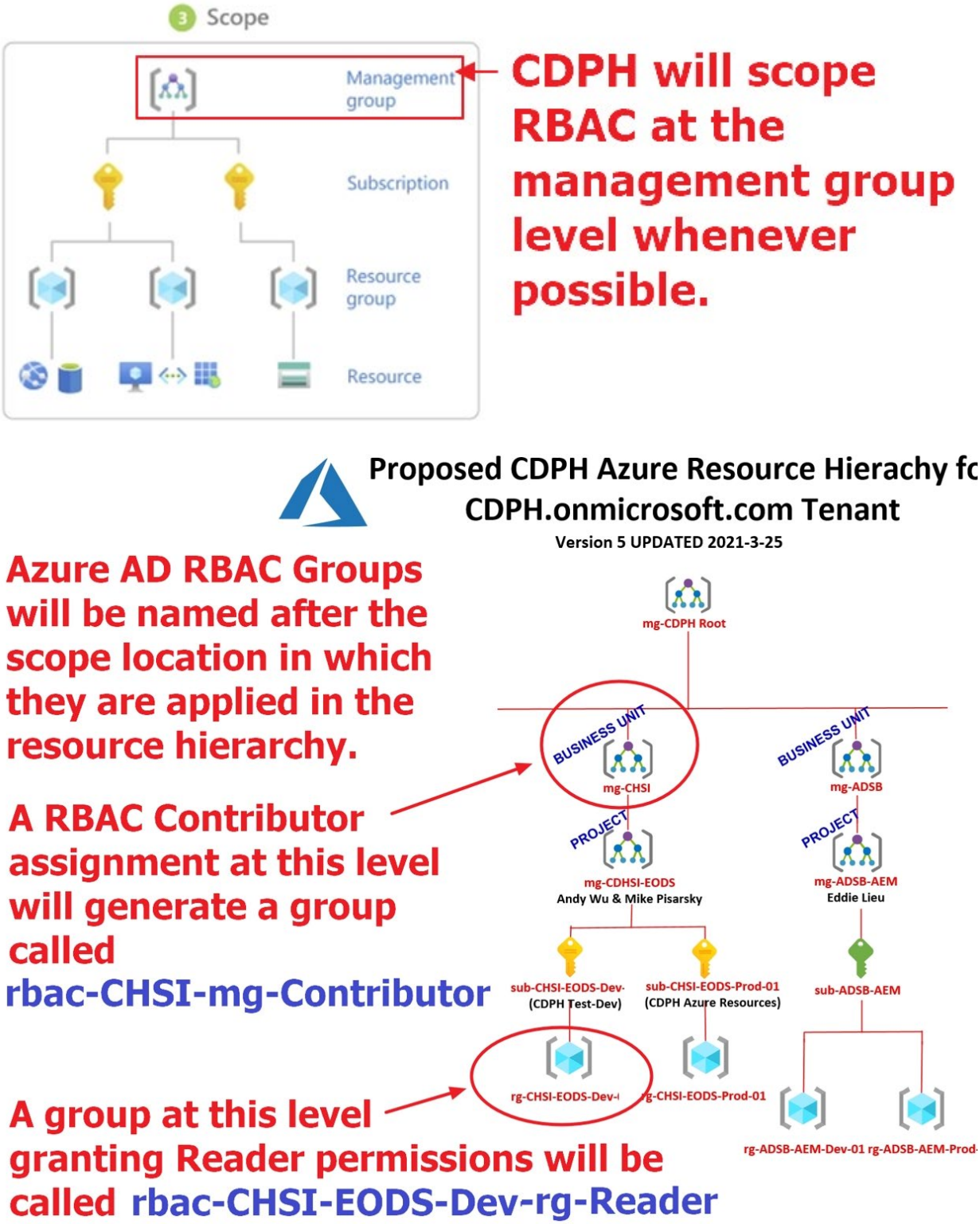
REFERENCE:

From: Subido, James@CDPH
Sent: Friday, June 18, 2021 11:14 AM
To: 'Moturu, Uma Maheswara Rao' <umoturu@deloitte.com>
Cc: Mathew, Beulah@CDPH <Beulah.Mathew@cdph.ca.gov>; Kochkin, Ievgen <ikochkin@deloitte.com>; Jain, Isha <ishajain@deloitte.com>; Benson, Tyrone@CDPH <Tyrone.Benson@cdph.ca.gov>; Wu, Andy@CDPH <Andy.Wu@cdph.ca.gov>
Subject: Azure AD Groups for Delegating Power Platform/Dynamics Privileges

Hello Mahesh,
Andy, Tyrone, and I came up with the following naming convention for Enterprise App delegation of privileges. Please let me know if you have any questions. Thanks, James

Role	Role Type	Activities	Owner	Members	Azure AD GROUP
Global Admin	Out of the box	Add Licenses Add Security Roles Create users Backup and restore Reset password for all users Add and manage domains Capacity limits (Data, flows, users etc per environment) Tenant level log reviews and monitoring	ITSD	TBD	rbac-GDSP-SIS-ea-PowerPlatform-GlobalAdmin
System Administrator	Out of the box	Customization or Administration of the environment Perform Admin functions Manage Security Roles View all data in the environment	SIS Team	Mahesh Moturu Isha Jain Ievgen Kochkin	rbac-GDSP-SIS-ea-PowerPlatform-SystemAdmin
System Customizer	Out of the box	Environment Customization (can view only the records for environment	SIS Team	Sangbaran Chakraborthy Anusha Bhuma Krunal Parmar Zack Sheaman Prateik Dubey Purushotham Subbella <We will add more...>	rbac-GDSP-SIS-ea-PowerPlatform-SystemCustomer
Environment Maker	Out of the box	Within the environment can create new resources, including: Apps Connections Custom APIs Gateways Flows using Power Automate (this role doesn't have priveleges to access data within an environment)	SIS Team	Sangbaran Chakraborthy Anusha Bhuma Krunal Parmar Zack Sheaman Prateik Dubey Purushotham Subbella <We will add more...>	rbac-GDSP-SIS-ea-PowerPlatform-EnvironmentMake

Scoping RBAC delegation at the management group level maximizes security and minimizes administrative overhead. Scoping at the Resource Group level may be required for more granular delegation. Whenever possible, avoid scoping at the resource level.



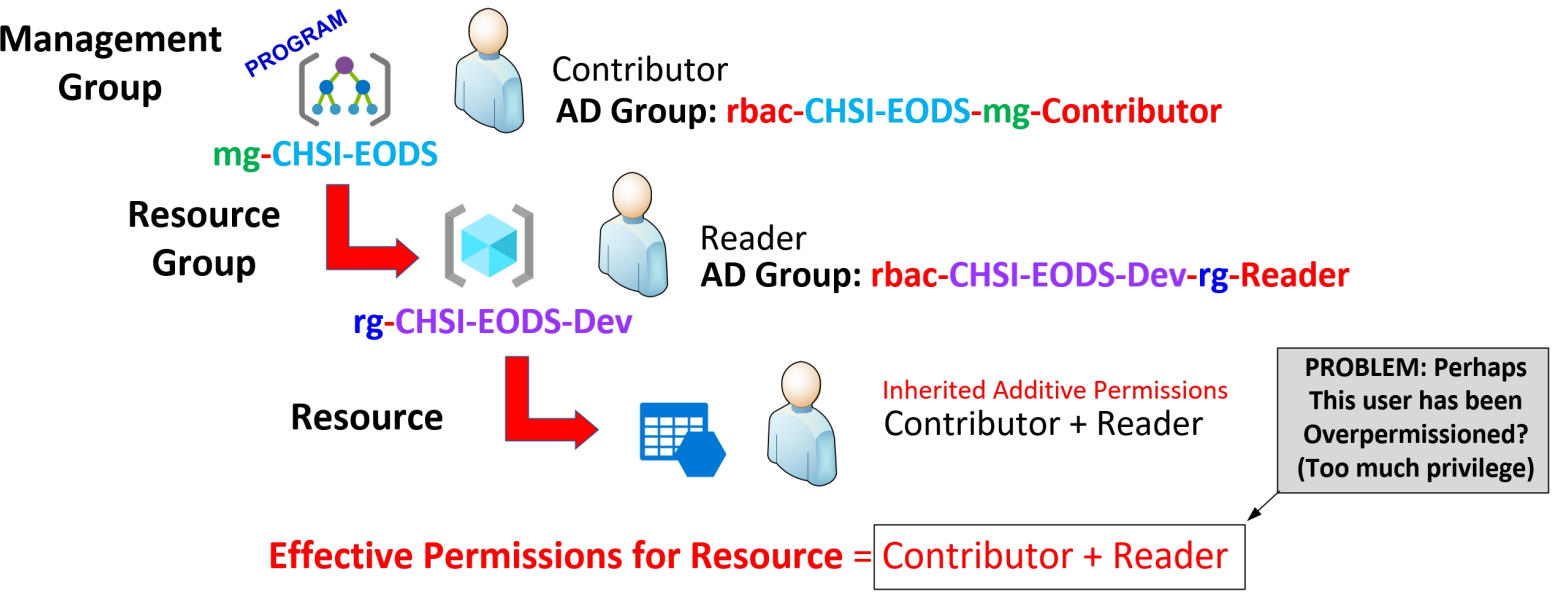
Here are additional examples:

Azure AD Group for RBAC Name	Description
rbac-CDPH-Root-mg-Reader	Reader RBAC role assignment for the root level management group (mg).

rbac-ADSB-AEM-mg-LogAnalyticsContributor	Log Analytics Contributor RBAC role assignment scoped at the ADSB-AEM management group (mg).
rbac-CHSI-EODS-Dev-dbw-Owner	Azure Databricks Service Workspace (dbw) Owner RBAC role assignment scoped at the resource level.
rbac-CHSI-EODS-Prod-rg-Reader	Reader RBAC role assignment scoped at the CHSI-EODS-Prod-01 resource group (rg).

EASIER RBAC AUDITING THROUGH GROUP NAMING CONVENTION

In the example below, the fact that the user is a member of two groups that both begin with "**rbac-CHSI-EODS**" is a **RED FLAG that raises suspicion:** Is the user below inheriting more privileges than necessary? Is the intended security posture Reader only for the resource?



COMPELLING ADVANTAGES GAINED WITH AZURE AD RBAC GROUP NAMING CONVENTION:

- Just by looking at the name of the Azure AD Group, one can very easily determine the following critical information:
    - Owner of the resources
    - The level in the resource hierarchy in which it is applied
    - The resources for which the assignment is intended to secure
    - The actual RBAC role assignment,
    - Whether or not it is a custom role (Custom roles might possibly present more risk and will always require more validation work since a custom role that works today may not continue to work six months from now in the dynamic world of Azure).
- Since RBAC flows down the resource hierarchy, the source of an inherited role will be readily and easily determined. This makes auditing permissions, which is normally bewilderingly time consuming, a much easier process to accomplish.
- RBAC auditing for changes is easier since any event in the Activity Log and Azure AD Audit Log that is prefixed by "rbac-"means that a change to RBAC role assignments occurred.
- The naming convention lends itself very easily for Identity Governance Access Review delegation to business unit managers (who may not be technical). Each business unit manager will readily understand the purpose for any given staff's membership just by looking at the name of a given Azure AD RBAC group and recertify the continued need for that groups membership or deny the membership.
- ***"Do I need to create a new Azure AD Group, or can I use an existing one?"*** will be easy to answer since all groups relating to a business unit or business unit program will "float" together.

REFERENCE: April 1, 2021 Audit of All Existing RBAC Role Assignments

The following inventory of existing RBAC role assignments was conducted on April 1, 2021 with the goal of understanding existing assignments so that a naming convention and strategy for replacing individual user accounts with Azure Active Directory groups could be developed.

Here is a partial list of the audit results, with AD Groups highlighted in yellow.

	ObjectTy	DisplayName	SignInName	RoleDefinitionName	PROPOSED AZURE AD Group	Scope
2	User	Alan Haley	ahaley@cdph.onmicrosoft.com	Application Insights Component Contributor	rbac-ADSB-AEM-mg-ApplicationInsightsComponentContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
3	User	Alan Haley	ahaley@cdph.onmicrosoft.com	Application Insights Snapshot Debugger	rbac-ADSB-AEM-mg-ApplicationInsightsSnapshotDebugger	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
4	User	Alan Haley	ahaley@cdph.onmicrosoft.com	Log Analytics Contributor	rbac-ADSB-AEM-mg-LogAnalyticsContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
5	User	Alan Haley	ahaley@cdph.onmicrosoft.com	Monitoring Contributor	rbac-ADSB-AEM-mg-MonitoringContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
6	User	Andy Wu	awu@cdph.onmicrosoft.com	Contributor	rbac-CHSI-EODS-Dev-01-rg-Contributor	SUBSCRIPTION-CDPH Test-Dev
7	User	Andy Wu	awu@cdph.onmicrosoft.com	Owner	REDUNDANT	SUBSCRIPTION-Microsoft Azure Enterprise
8	User	Calvin Lee	clee@cdph.onmicrosoft.com	Contributor	rbac-CHSI-EODS-mg-Contributor	SUBSCRIPTION-CDPH Azure Resources
9	User	Calvin Lee	clee@cdph.onmicrosoft.com	Contributor	REDUNDANT	SUBSCRIPTION-Microsoft Azure Enterprise
10	User	Calvin Lee	clee@cdph.onmicrosoft.com	Owner	ASK TYRONE: SOSS Contributor or Owner at root level?	SUBSCRIPTION-CDPH Azure Resources/resourceGroups/CDPH-SOSS-SASS
11	User	Calvin Lee	clee@cdph.onmicrosoft.com	Owner	rbac-CDPH-Root-mg-Owner	SUBSCRIPTION-CDPH Azure Resources/resourceGroups/CDPH-DataBricks-Test-Pu
12	User	Calvin Lee	clee@cdph.onmicrosoft.com	Owner	REDUNDANT	SUBSCRIPTION-CDPH Test-Dev
13	User	Calvin Lee	clee@cdph.onmicrosoft.com	Owner	REDUNDANT	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
14	User	Calvin Lee	clee@cdph.onmicrosoft.com	Support Request Contributor	REDUNDANT	SUBSCRIPTION-Microsoft Azure Enterprise
15	User	Chu, Wing@CDPH	Wing.Chu@cdph.ca.gov	Contributor	rbac-CHSI-EODS-Dev-01-rg-Contributor	SUBSCRIPTION-CDPH Test-Dev
16	User	Dan D'Arcangelis (Admin)	dan.dArcangelis@cdph.onmicrosoft.com	Application Insights Component Contributor	rbac-ADSB-AEM-mg-ApplicationInsightsComponentContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
17	User	Dan D'Arcangelis (Admin)	dan.dArcangelis@cdph.onmicrosoft.com	Application Insights Snapshot Debugger	rbac-ADSB-AEM-mg-ApplicationInsightsSnapshotDebugger	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
18	User	Dan D'Arcangelis (Admin)	dan.dArcangelis@cdph.onmicrosoft.com	Log Analytics Contributor	rbac-ADSB-AEM-mg-LogAnalyticsAnalyticsContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
19	User	Dan D'Arcangelis (Admin)	dan.dArcangelis@cdph.onmicrosoft.com	Monitoring Contributor	rbac-ADSB-AEM-mg-MonitoringContributorMonitoringContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
20	User	Daugherty, Daniel@CDPH	Daniel.Daugherty@cdph.ca.gov	Contributor	rbac-CHSI-EODS-Dev-01-rg-Contributor	SUBSCRIPTION-CDPH Azure Resources/resourceGroups/CDPH-DataBricks-Test-Pu
21	User	David Lindauer	dlindauer@cdph.onmicrosoft.com	Application Insights Component Contributor	rbac-ADSB-AEM-rg-ApplicationInsightsComponentContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
22	User	David Lindauer	dlindauer@cdph.onmicrosoft.com	Application Insights Snapshot Debugger	rbac-ADSB-AEM-rg-ApplicationInsightsSnapshotDebugger	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
23	User	David Lindauer	dlindauer@cdph.onmicrosoft.com	Log Analytics Contributor	rbac-ADSB-AEM-mg-LogAnalyticsContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
24	User	David Lindauer	dlindauer@cdph.onmicrosoft.com	Monitoring Contributor	rbac-ADSB-AEM-rg-MonitoringContributorMonitoringContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
25	Group	EODS-Admin-Dev		Owner	rbac-CHSI-EODS-Dev-01-rg-Owner	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Dev-EODS-Databricks-priva
26	Group	EODS-Admin-Dev		Storage Blob Data Contributor	CONFLICTING (See Owner Role Above)	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Dev-EODS-Databricks-priva
27	Group	EODS-DAAD-Analyst-Dev-NonAdmin		Reader	RESOURCE LEVEL ASSIGNMENT: Is this necessary?	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Dev-EODS-Databricks-priva
28	Group	EODS-DAAD-Engineer-Dev-Admin		Reader	RESOURCE LEVEL ASSIGNMENT: Is this necessary?	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Dev-EODS-Databricks-priva
29	Group	EODS-Developer-Dev		Contributor	rbac-CHSI-EODS-Dev-01-rg-Contributor	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Dev-EODS-Databricks-priva
30	Group	EODS-Developer-Dev		Storage Blob Data Contributor	rbac-CHSI-EODS-Dev-01-rg-StorageBlobDataContribor	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Dev-EODS-Databricks-priva
31	Group	EODS-SAAD-Analyst-Dev-Private-Cannabis		Storage Blob Data Owner	rbac-CHSI-EODS-Dev-o1-rg-StorageBlobDataOwner	SUBSCRIPTION-CDPH Test-Dev/resourceGroups/CDPH-Stage-EODS-Databricks-pri
32	User	Eric Abeyta	EAbeyta@cdph.onmicrosoft.com	Contributor	ASK TYRONE	SUBSCRIPTION-CDPH Azure Resources/resourceGroups/CDPH-SOSS-SASS/provide
33	User	Eric Abeyta	EAbeyta@cdph.onmicrosoft.com	Reader	rbac-CHSI-EODS-mg-Reader	SUBSCRIPTION-CDPH Azure Resources
34	User	Frederick Spies	frspies@microsoft.com	Reader	rbac-CHSI-EODS-mg-Reader	SUBSCRIPTION-CDPH Azure Resources
35	User	Fujimoto, Scott@CDPH	Scott.Fujimoto@cdph.ca.gov	Reader	rbac-CHSI-EODS-Dev-01-rg-Reader	SUBSCRIPTION-CDPH Azure Resources/resourceGroups/CDPH-DataBricks-Test-Pu
36	User	Giles, Theresa@CDPH	Theresa.Giles@cdph.ca.gov	Contributor	rbac-CHSI-EODS-mg-Contributor	SUBSCRIPTION-CDPH Azure Resources
37	User	Harvey Hayes	hhayes@cdph.onmicrosoft.com	Application Insights Component Contributor	rbac-ADSB-AEM-rg-ApplicationInsightsComponentContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
38	User	Harvey Hayes	hhayes@cdph.onmicrosoft.com	Application Insights Snapshot Debugger	rbac-ADSB-AEM-rg-ApplicationInsightsSnapshotDebugger	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
39	User	Harvey Hayes	hhayes@cdph.onmicrosoft.com	Log Analytics Contributor	rbac-ADSB-AEM-rg-LogAnalyticsAnalyticsContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
40	User	Harvey Hayes	hhayes@cdph.onmicrosoft.com	Monitoring Contributor	rbac-ADSB-AEM-rg-MonitoringContributorMonitoringContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
41	User	Ian Sanford (Admin)	isanford@cdph.onmicrosoft.com	Owner	rbac-CHSI-EODS-mg-Owner	SUBSCRIPTION-CDPH Azure Resources
42	User	Ian Sanford (Admin)	isanford@cdph.onmicrosoft.com	Owner	REDUNDANT	SUBSCRIPTION-CDPH Test-Dev
43	User	Ian Sanford (Admin)	isanford@cdph.onmicrosoft.com	Support Request Contributor	rba-ADSB-mg-SupportRequestContributor	SUBSCRIPTION-Microsoft Azure Enterprise
44	User	Jaime Silvano	jsilvano@cdph.onmicrosoft.com	Contributor	rbac-CHSI-EODS-Dev-01-rg-Contributor	SUBSCRIPTION-CDPH Test-Dev
45	User	Jaime Silvano	jsilvano@cdph.onmicrosoft.com	Reader	rbac-CHSI-EODS-mg-Reader	SUBSCRIPTION-CDPH Azure Resources
46	User	Jaime Silvano	jsilvano@cdph.onmicrosoft.com	Support Request Contributor	rba-ADSB-mg-SupportRequestContributor	SUBSCRIPTION-Microsoft Azure Enterprise
47	User	Janet French	jfrench@cdph.onmicrosoft.com	Reader	rbac-CDPH-Root-mg-Reader	SUBSCRIPTION-CDPH Test-Dev
48	User	Janet French	jfrench@cdph.onmicrosoft.com	Reader	REDUNDANT	SUBSCRIPTION-CDPH Azure Resources
49	User	Janet French	jfrench@cdph.onmicrosoft.com	Reader	REDUNDANT	SUBSCRIPTION-Microsoft Azure Enterprise
50	User	Jared Letendre	JLetendre@cdph.onmicrosoft.com	Application Insights Component Contributor	rbac-ADSB-AEM-rg-ApplicationInsightsComponentContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
51	User	Jared Letendre	JLetendre@cdph.onmicrosoft.com	Application Insights Snapshot Debugger	rbac-ADSB-AEM-rg-ApplicationInsightsSnapshotDebugger	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
52	User	Jared Letendre	JLetendre@cdph.onmicrosoft.com	Log Analytics Contributor	rbac-ADSB-AEM-rg-LogAnalyticsAnalyticsContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
53	User	Jared Letendre	JLetendre@cdph.onmicrosoft.com	Monitoring Contributor	rbac-ADSB-AEM-rg-MonitoringContributorMonitoringContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
54	User	Jeffrey Kolek	jkolek@cdph.onmicrosoft.com	Application Insights Component Contributor	rbac-ADSB-AEM-rg-ApplicationInsightsComponentContributor	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS
55	User	Jeffrey Kolek	jkolek@cdph.onmicrosoft.com	Application Insights Snapshot Debugger	rbac-ADSB-AEM-rg-ApplicationInsightsSnapshotDebugger	SUBSCRIPTION-Microsoft Azure Enterprise/resourceGroups/RG-ADSB-PHATS

RESULT OF RBAC AUDIT OF APRIL 1, 2021: These 24 New Azure AD RBAC Groups will be created to replace individual user account RBAC assignments:

1	rbac-ADSB-AEM-rg-ApplicationInsightsComponentContributor
2	rbac-ADSB-AEM-rg-ApplicationInsightsSnapshotDebugger
3	rbac-ADSB-AEM-rg-LogAnalyticsAnalyticsContributor
4	rbac-ADSB-AEM-rg-MonitoringContributorMonitoringContributor
5	rbac-ADSB-AEM-mg-ApplicationInsightsComponentContributor
6	rbac-ADSB-AEM-mg-ApplicationInsightsSnapshotDebugger
7	rbac-ADSB-AEM-mg-LogAnalyticsAnalyticsContributor
8	rbac-ADSB-AEM-mg-LogAnalyticsContributor
9	rbac-ADSB-AEM-mg-MonitoringContributor
10	rbac-ADSB-AEM-mg-MonitoringContributorMonitoringContributor
11	rbac-ADSB-mg-SupportRequestContributor
12	rbac-ADSB-mg-LogAnalyticsContributor
13	rbac-CDPH-Root-mg-Owner
14	rbac-CDPH-Root-mg-Reader
15	**rbac-CHSI-EODS-Dev-dbw-Owner (NOTE: dbw = Databricks Workspace)**
16	rbac-CHSI-EODS-Dev-rg-Contributor
17	rbac-CHSI-EODS-Dev-rg-Owner
18	rbac-CHSI-EODS-Dev-rg-Reader
19	rbac-CHSI-EODS-Dev-rg-StorageBlobDataContribor

20	rbac-CHSI-EODS-Dev-o1-rg-StorageBlobDataOwner
21	rbac-CHSI-EODS-mg-Contributor
22	rbac-CHSI-EODS-mg-LogAnalyticsContributor
23	rbac-CHSI-EODS-mg-Owner
24	rbac-CHSI-EODS-mg-Reader

NAMING CONVENTION: Custom RBAC Roles

Role-based access control (RBAC) is an integral component of the governance framework. It ensures that only authorized and approved users have appropriate access to resources. Azure provides predefined (built-in) roles that are available to CDPH

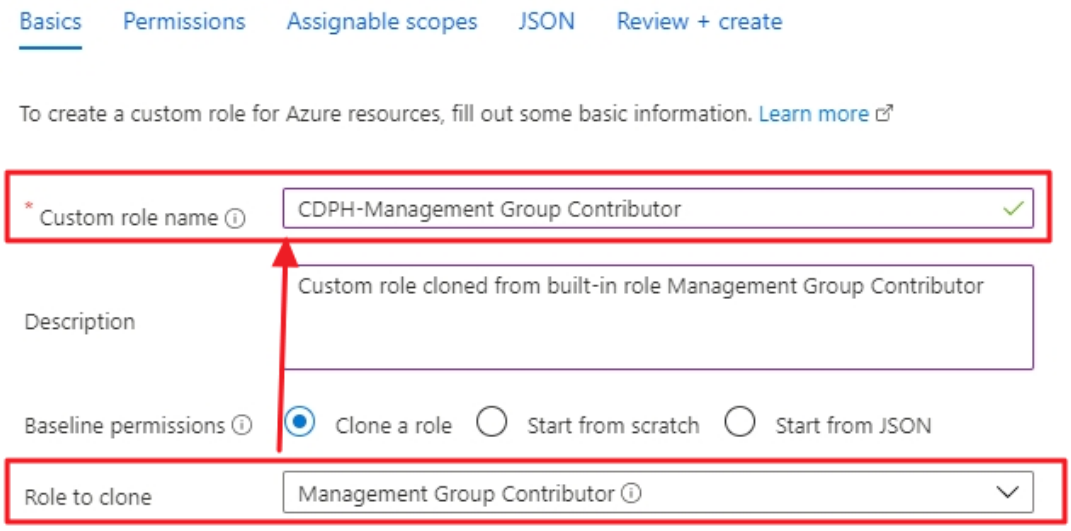
Custom Role Name: CDPH-Management Group Contributor

All custom roles created by CDPH

Source Policy Name

Naming Component	Description
Prefix	All custom roles created by CDPH will bear the prefix of "CDPH" to distinguish it from the built-in roles in Azure.
Source Built-in Role Name	While CDPH can create a custom role from scratch, it would be much easier to clone the closest existing built-in role and customize it instead. The name of the source built-in Azure role will be used for naming. Doing so documents the origin of the custom role.

NAMING CONVENTION: Custom role will be named from the originating built-in role from which it was cloned.

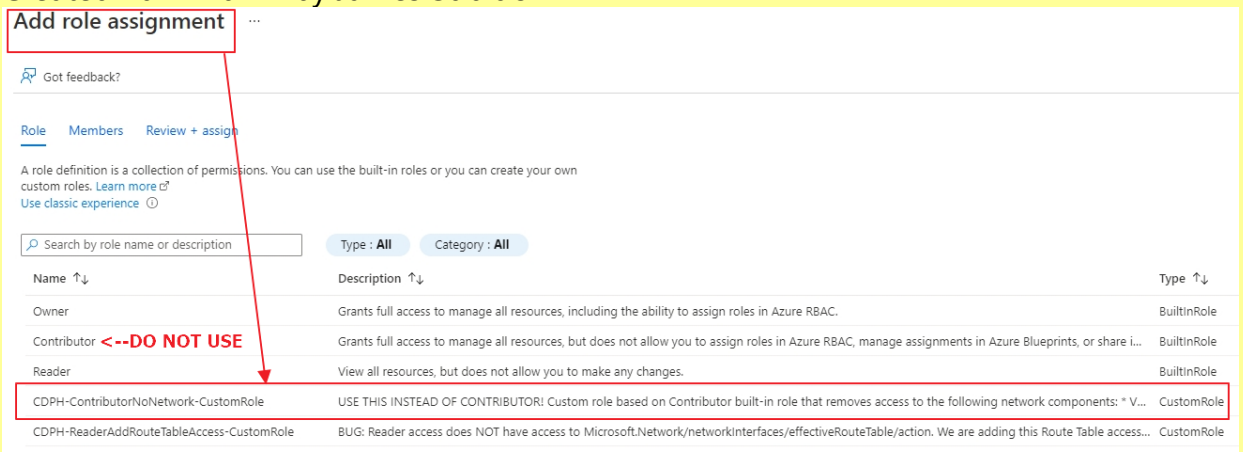


UPDATE: December 15, 2021: Replacement of Contributor Built-In Role

USE THIS INSTEAD OF CONTRIBUTOR! Azure's built in Contributor role delegates too many privileges. Instead of using Contributor, use the custom role called "CDPH-ContributorNoNetwork-CustomRole". It is based on the Contributor built-in role but removes access to the following network components:

- VNets and Subnets
- Network Security Groups
- Route Tables

Created 2021-10-21 by James Subido



NAMING CONVENTION: Enterprise Apps and Service Accounts

Enterprise App Name: sa-CID-IB-DVRRemediation

Prefix | Owner | Application

Service Account Name: sa-CID-IB-DVRRemediation-Snowflake-JohnSmith-Dev@cdph.onmicrosoft.com

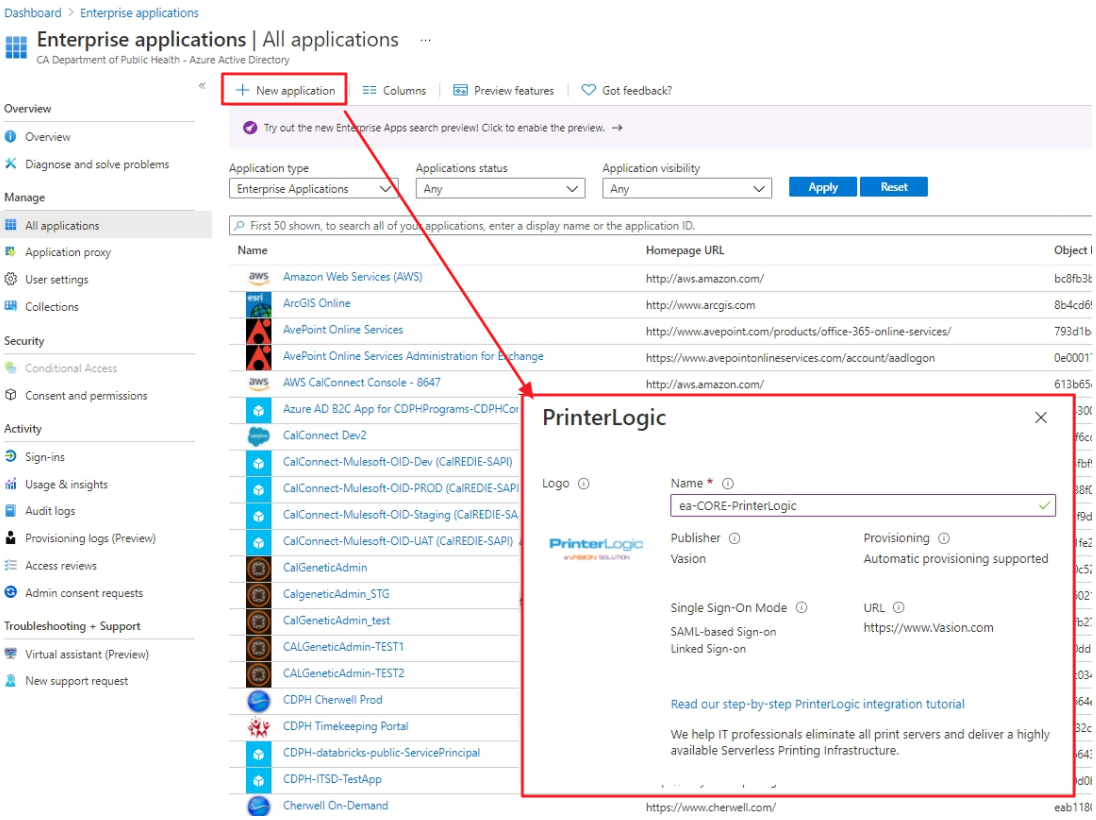
Prefix | Owner | Application | Purpose | Name | Environment | Email Suffix

Please note that Service Accounts have a limit of 64 characters BEFORE the @ symbol. The service account in the example given above for DVRRemediation, is using 48 characters.

Description	Example
DVR Remediation in Snowflake Dev environment	sa-CID-IB-DBRRemediation-Snowflake-JohnSmith-Dev@cdph.onmicrosoft.com
Santa Barbara Snowflake Account (External entity that requires a service account).	sa-CID-IB-SantaBarbara-Snowflake-John.Smith-Prod@cdph.onmicrosoft.com
CalConnect Tableau User for the Informatics Branch Snowflake (no dev and prod environment)	sa-CID-DCDC-CalConnectTableau-Snowflake-John.Smith-Prod@cdph.onmicrosoft.com

NAMING CONVENTION: Enterprise Applications

Enterprise Applications are a different class of resource since they do not belong to a Resource Group nor do they support tagging. The naming convention will focus on ownership, which will provide the advantage of accountability: To whom do we go if we have any questions regarding this application?

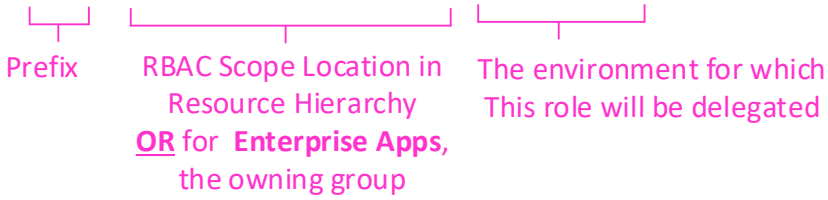


Naming Component	Description
Prefix	Enterprise Applications will begin with the prefix (ea).
CDPH Business Unit	The business unit which owns the Enterprise Application. The example shows CORE, which indicates it is part of the CORE Azure Resources managed by ITSD.
Name	The actual unchanged name of the Enterprise Application.

NAMING CONVENTION: Key Vault

Key Vaults are highly security sensitive Azure resources in that they are essential in storing encryption keys and secrets which are used to protect data in the cloud.

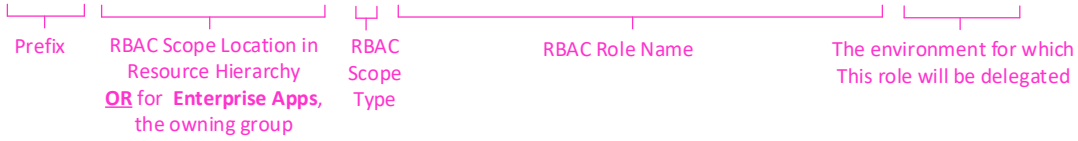
Key Vault Name: kv-IB-CAIR2-IRIS-Dev-01



Naming Component	Description
Prefix	Key Vault abbreviates to (kv)
CDPH Business Unit	The business unit who owns the management group.
CDPH Business Unit Program	The specific program, application, or workload associated with the subscription.
Environment	• (Dev) - Development • (Stag) - Staging • (Prod) - Production

Delegating privileges is essential for security sensitive Key Vaults. To delegate permission, use the following naming convention for the RBAC group:

FOR DELEGATING PERMISSIONS: Key Vault Azure Active Directory Group Name: rbac-IB-CAIR2-IRIS-ir-KeyVaultCertificatesOfficer-Dev-01



For additional information, please see the next section "Azure AD Groups for RBAC Assignments".

NAMING CONVENTION: Policies

Policies are associated with three naming categories:

- Policy definition name
- Policy assignment name

- Policy category
- Policy exceptions

Microsoft Azure provides built-in policies under multiple default categories. These policies are not preassigned. CDPH can assign these policies and only worry about the assignment names. A recommended practice is for CDPH to create its own categories and policies before assigning. This enables CDPH the flexibility to implement its own naming standards and control any customizations, while simultaneously maintaining a library of the default policies as a template artifact.

Policy Definition Name and Policy Category Name

Policy Name: CDPH-Tag resource with Owner Name and Date

CDPH- : All custom policies created by CDPH

Tag resource with Owner Name and Date : Policy name

Policy Category: CDPH-Under Review

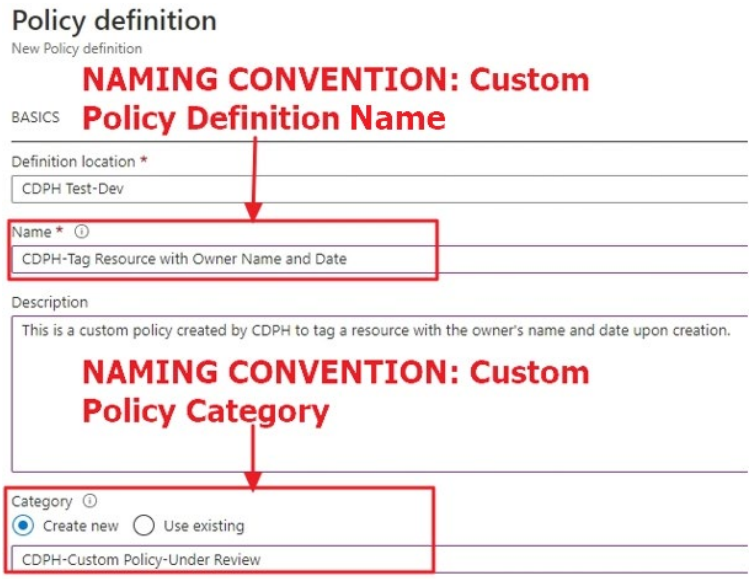
CDPH- : All custom policies created by CDPH

Under Review : Policy status

Naming Component	Description
Policy Prefix	• (CDPH-) All custom policies created by CDPH will bear the prefix of "CDPH-" to distinguish it from the hundreds of built-in policies created by Azure.
Policy Name	The name of the policy. If based on an existing built-in Azure policy, simply copy the name of the originating Azure policy to document the source policy.
Policy Suffix (Categories only)	When assigning a policy, denoting its status as "Under Review" or "Production" or "Production with Exemptions" are the options to consider. • (Under Review) – Running in audit-only mode, policy is being assessed for its impact to the environment. • (Production) – Policy is being enforced. Violators are denied resources.

	• (Production with Exceptions) - Policy is being enforced. Violators are denied resources except for those with waivers.

The process of defining a custom policy name and custom category are performed during the step of creating a policy definition (screen shot below). CDPH can edit the name and category of the policy by using the editing option. Note that once a category has been created, CDPH can simply select Use Existing Option to pick a previously created category.



Assignment naming standards can denote whether a given policy is in audit only mode or in enforcement mode. Audit only will provide CDPH with a compliance assessment. In contrast, a policy that is enforced will deny resources. Prior to deploying a policy, best practice states to initially deploy it in audit only mode with the category of "CDPH-Under Review" as discussed previously. This step will provide CDPH the ability to assess the impact of a new policy and provide the opportunity to remediate the issues that come to light prior to its enforcement.

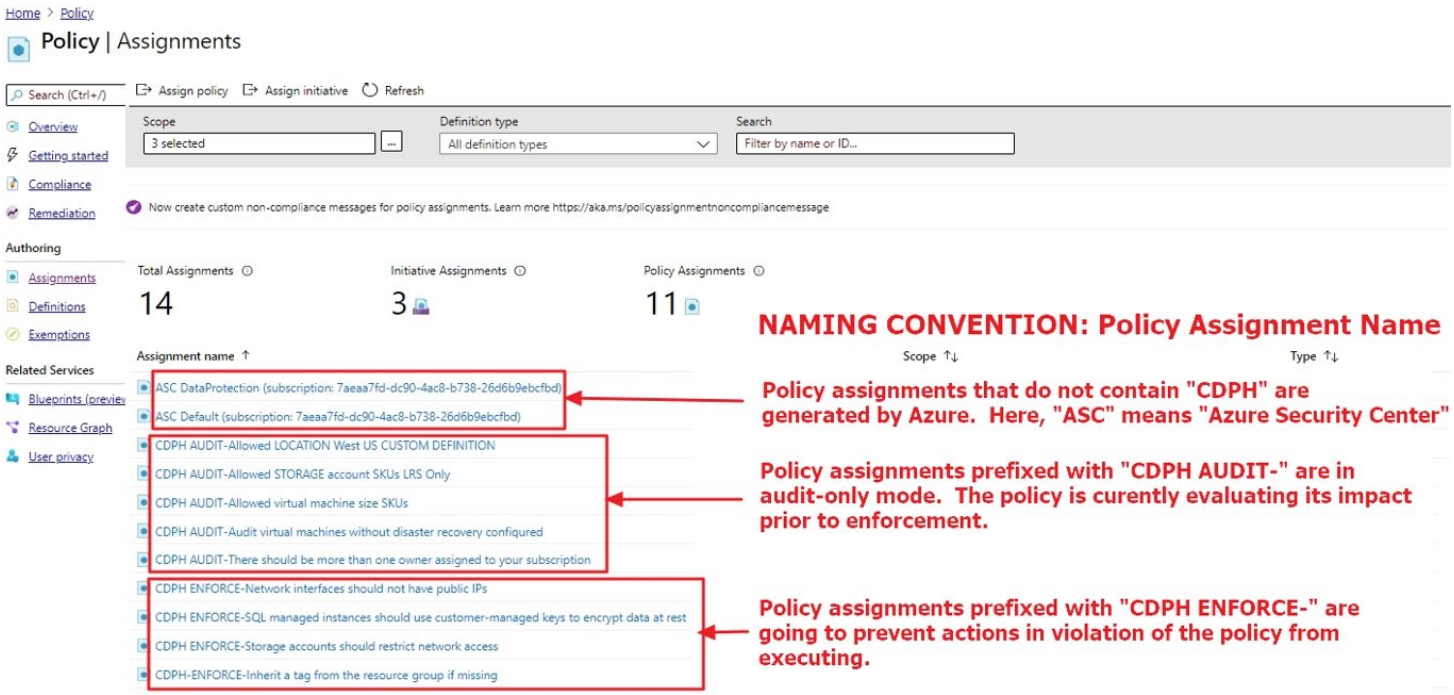
Policy Assignment Name

Policy Assignment: CDPH-Audit-Tag resource with Owner Name and Date

- CDPH- : All custom policies created by CDPH
- Audit- : Policy enforcement status
- Tag resource with Owner Name and Date : Policy name

Naming Component	Description
Policy Prefix	• (CDPH) - All custom policies created by CDPH will bear the prefix of "CDPH-" to distinguish it from the hundreds of built-in policies created by Azure. • (ASC) – This prefix is automatically applied by policies assigned through Azure Security Center.
Policy Enforcement Status	The enforcement status will identify the policy in either auditing mode or enforcement mode. Auditing will allow CDPH the ability to assess the impact of the policy prior to its enforcement, which will deny resources in the event of a policy violation. • (Audit) - assess the impact of the policy prior to its enforcement • (Enforced) - deny resources in the event of a policy violation
Policy Name	The name of the policy. If based on an existing built-in Azure policy, simply copy the name of the originating Azure policy to document the source policy.

The screen shot below highlights how the naming convention fits in when all available assignments are viewed. Note that Azure Security Center assignments are prefixed with "ASC" and thus float on top of the list. Followed by "CDPH-AUDIT", this group of policies identify which policies are under review and impact assessment. Lastly, "CDPH-ENFORCED" identify the policies that are in production. This naming standard gives a clear view of the status of each policy.



Policy Exemption Name

In the event CDPH encounters a resource hierarchy or individual resource that will be exempted from a given policy, the Azure Policy exemptions feature is available to be used. Resources that are exempt will count toward compliance.

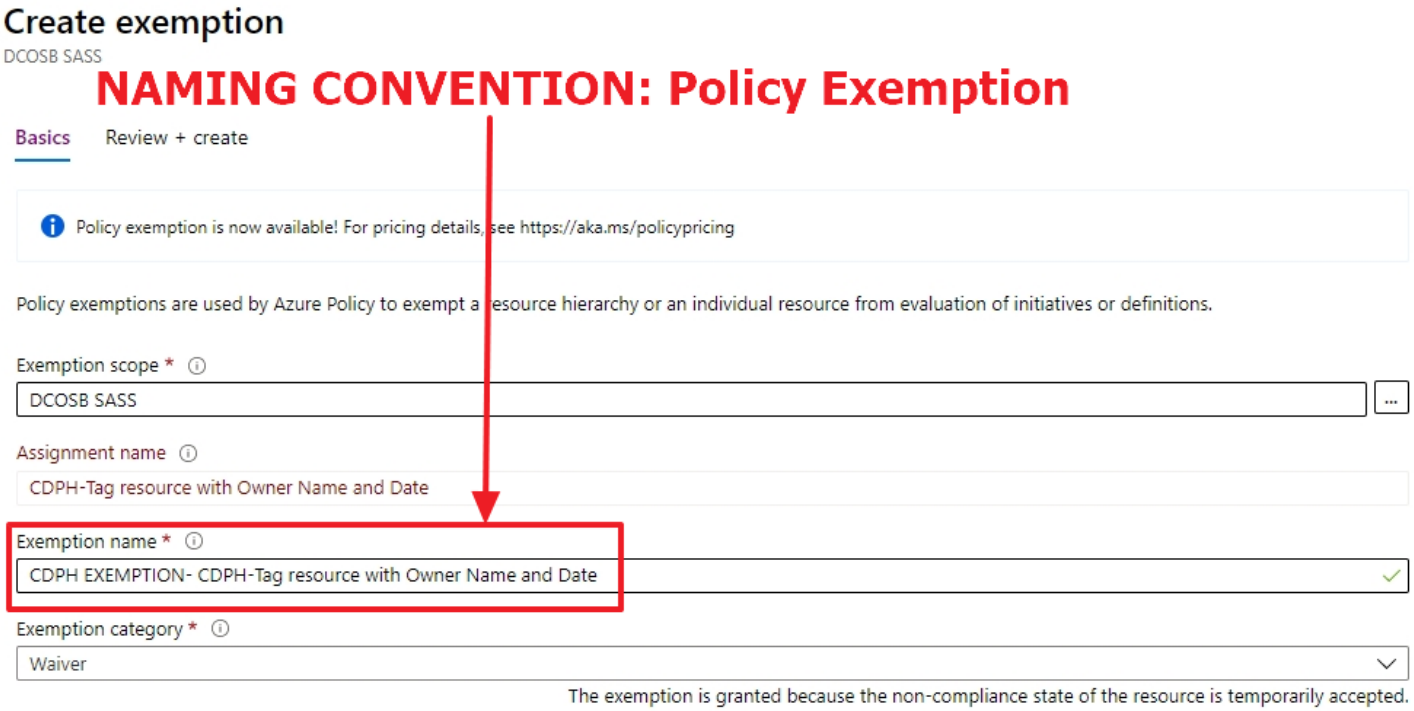
Policy Exemption: CDPH-EXEMPTION-CDPH-Tag resource with Owner Name and Date

All exemptions created by CDPH

Name of policy

Naming Component	Description
Policy Prefix	• (CDPH-EXEMPTION) All exemptions created by CDPH will use this prefix
Policy Name	The name of the policy. If based on an existing built-in Azure policy, simply copy the name of the originating Azure policy to document the source policy.

The screen shot below provides the opportunity to rename the policy to conform to the naming standard. Note that by default, exemptions will be named with the subscription as the prefix followed by the name of the policy for which the exemption will apply.



The naming standards provide a clear view of the purpose, status, and disposition of CDPH's policies.

NAMING CONVENTION: Initiatives

Initiatives allow CDPH to group several policies cohesively in order to deliver a consistent compliance policy for specific governance and regulatory compliance objectives.

Initiatives are associated with three naming categories:

- Initiative definition name
- Initiative assignment name
- Initiatives category

Azure provides built-in initiatives under multiple default categories. These initiatives are unused and unassigned by default. A recommended practice is for CDPH to create its own categories and new custom initiatives that are planned, scoped, and assigned in line with its governance objectives.

Initiative Name: CDPH-INITIATIVE-HITRUST/HIPAA

Initiative Category: CDPH-INITIATIVE -Under Review

Initiative Assignment: CDPH-INITIATIVE-Audit-HITRUST/HIPAA

Naming Component	Description
Initiative Prefix	All custom initiatives created by CDPH will bear the prefix of "CDPH-INITIATIVE" to distinguish it from the built-in initiatives created by Azure.
Initiative Name	The name of the policy. If based on an existing built-in Azure policy, simply copy the name of the originating Azure policy to document the source policy.
Initiative Status	When assigning a policy, denoting its status as "Under Review" or "Production" or "Production with Exemptions" are the options to consider. • (Under Review) – Running in audit-only mode, policy is being assessed for its impact to the environment. • (Production) – Initiative is being enforced. Violators are denied resources. • (Production with Exceptions) - Initiative is being enforced. Violators are denied resources except for those with waivers.
Initiative Enforcement Status	The enforcement status will identify the initiative in either auditing mode or enforcement mode. Auditing will allow CDPH the ability to assess the impact of the initiative prior to its enforcement, which will deny resources in the event of a policy violation.

	• (Audit) - assess the impact of the initiative prior to its enforcement • (Enforced) - deny resources in the event of a policy violation

NAMING CONVENTION: Blueprints

Azure Blueprints makes it possible for CDPH to orchestrate the rapid build and deploy new environments while adhering to its defined requirements and governance compliance framework. While Blueprints can be saved to a management group or subscription, CDPH will use the root management groups as a standard practice for saving Blueprints for two reasons:

- Saving Blueprints on the CDPH root management group allows ALL child objects within the global hierarchy to use the Blueprints.
- Saving Blueprints on subscriptions provides difficulties in that subscriptions have a limited lifecycle – they could be tied into a business unit program which, at the end of the lifecycle, will be retired. Using management groups such as the root management group result

At the time of writing, Blueprints contain the following elements, called artifacts:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

The artifacts contained within Azure Blueprints inherit their naming convention. The naming standard consideration is as follows.

- Blueprint name
- Blueprint version
- Blueprint assignment name

The three areas depend on the life-cycle stage of the blueprint. The relevant life-cycle stages of the blueprint are creation and assignment. While editing a blueprint is allowed, renaming a blueprint is not. The name can be up to 48 characters (numbers and letters), with no spaces or special characters.

GOTCHA: At the time of this writing (February 2021), Blueprints cannot be renamed. A workaround is to create a new blueprint and use an export/import process. Additionally, Blueprint names do not allow spaces.

Blueprint Name: CDPH-BLUEPRINT-HIPAA

- CDPH-BLUEPRINT- : Prefix for blueprints created by CDPH
- HIPAA : Blueprint name

Blueprint Version: 1.3

- 1 : Major changes
- 3 : Minor changes

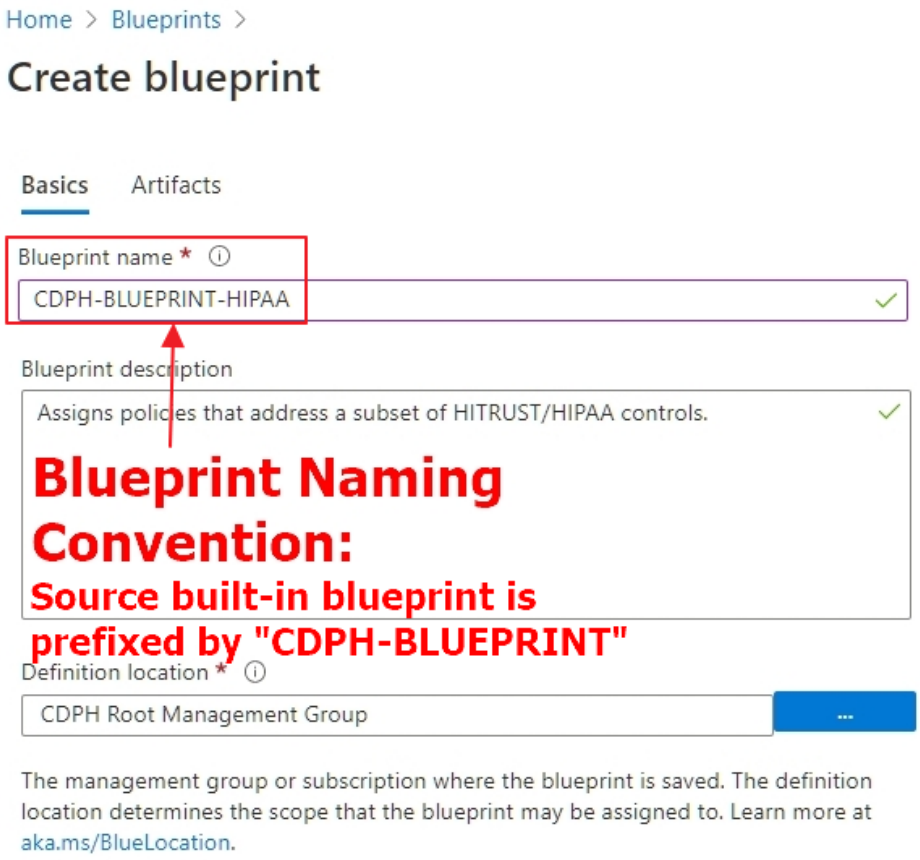
Blueprint Assignment: Assignment-CDPH-BLUEPRINT-HIPAA

- Assignment- : Prefix for assignments
- CDPH-BLUEPRINT- : Prefix for blueprints created by CDPH
- HIPAA : Blueprint name

Naming Component	Description
Blueprint Prefix	All blueprints created by CDPH will bear the prefix of "CDPH-BLUEPRINT "to distinguish it from the built-in blueprints created by Azure.
Blueprint Version	Each version of a blueprint is a unique object and can be individually published. As such, each version of a blueprint can also be deleted. Deleting a blueprint version does not have any impact on other versions of that blueprint. Major revisions: • (1.0) • (2.0) • (3.0) etc Minor Changes: • (1.1) • (1.2) • (1.3) etc
Blueprint Name	If based on an existing built-in Azure blueprint, simply copy the name of the originating Azure blueprint to document the source policy.

Blueprint Assignment Name	When assigning the blueprint, Azure generates an "Assignment" prefix. We will simply accept this default naming system. • (Assignment) Example: "Assignment-CDPH-BLUEPRINT-HIPAA"

When you initiate the creation of a blueprint, you are presented with the blueprint name field and description as shown in the screen shot below. Blueprints created by cloning an existing built-in blueprint such as HIPAA will simply inherit the name of the original blueprint in its name. For the example given below, since this is a blueprint based on the built-in Azure blueprint "HIPAA", we simply prefix it with "CDPH-BLUEPRINT" to come up with "CDPH-BLUEPRINT-HIPAA".

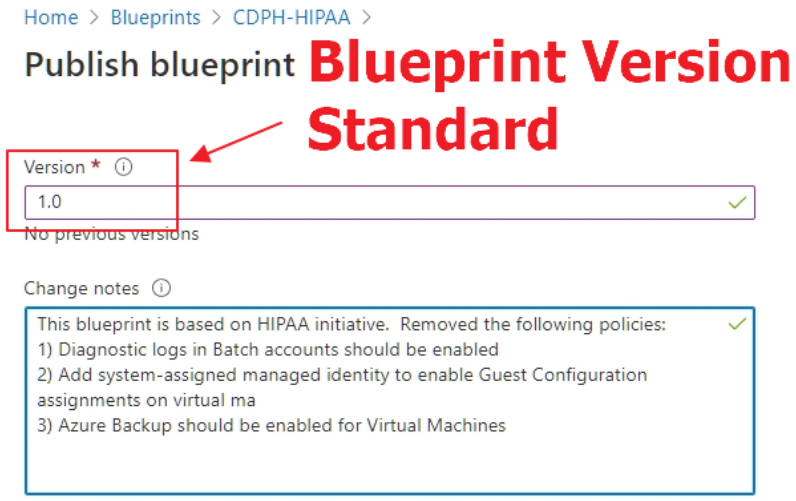


The next step to naming a blueprint is the version number. Blueprints created by default are saved as a draft and cannot be used until published. Publishing the blueprint requires assigning it.

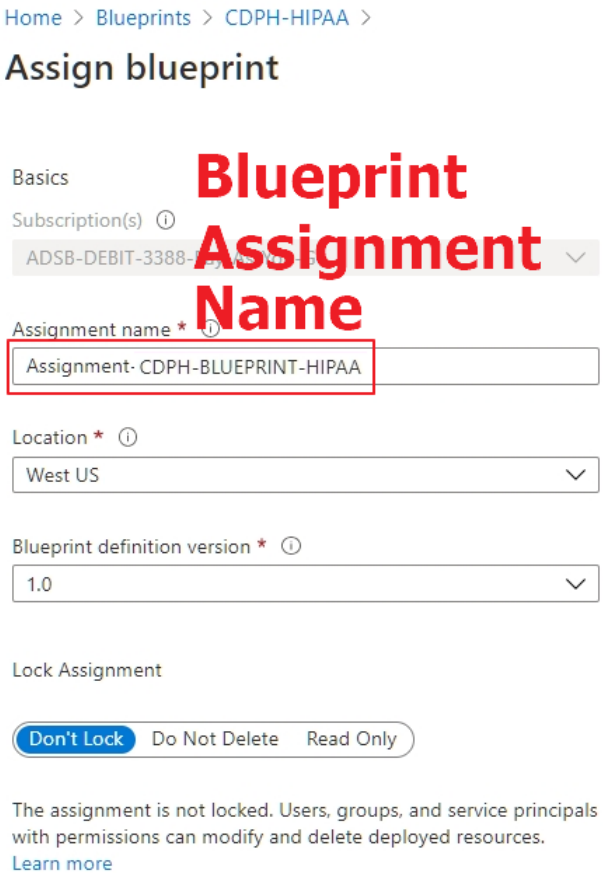
The publishing process requires a mandatory version. The version can be letters, numbers, and hyphens with a maximum length of 20 characters. The recommendation from Microsoft is to use a numbering notation similar to software versions, where the first number denotes a major version and

appended incremental numbers denote incremental versions. For example, 1.0 for the first version and 1.1 for the first minor change to the first version.

Blueprint version changes are seen in the Azure portal. The latest version of the blueprint is what is available in the blueprint definition code. The previous versions are visible and available when you initiate the assignment process.



The final name component is the assignment name. The naming convention will simply accept the default naming convention which provides an "Assignment-(*Blueprint name*)"



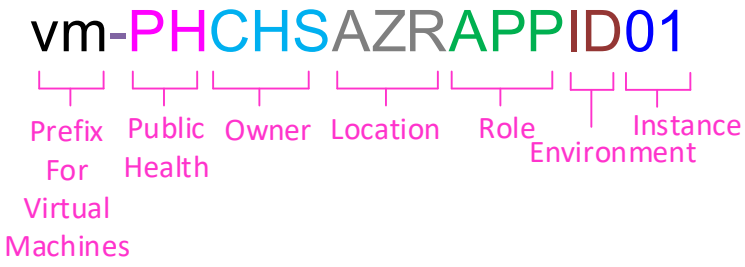
NAMING CONVENTION: Virtual Machines

CDPH has maintained a well-defined and accepted naming standard for the past several years. This section will propose that we simply repurpose the existing naming standard with the minor adjustment of prefixing the virtual machine name with a "vm". This would allow us to easily identify other ancillary Azure resources associated with the virtual machine such as public IP address, network interface card (NIC), network security group (NSG), and disks as belonging to a virtual machine and tying them all together as a logical bundle.

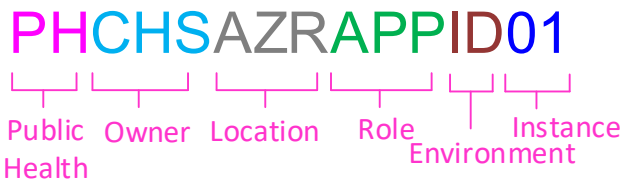
POLICY REMINDER: According to Tony Tran (April 19, 2021), he would like to minimize the deployment of VMs in the cloud as much as possible. Deploy VMs to the TMSP datacenter and deploy VMs to the cloud only when we have absolutely no other option.

REUSING EXISTING CDPH SERVER NAMING CONVENTION

Virtual Machine Name:

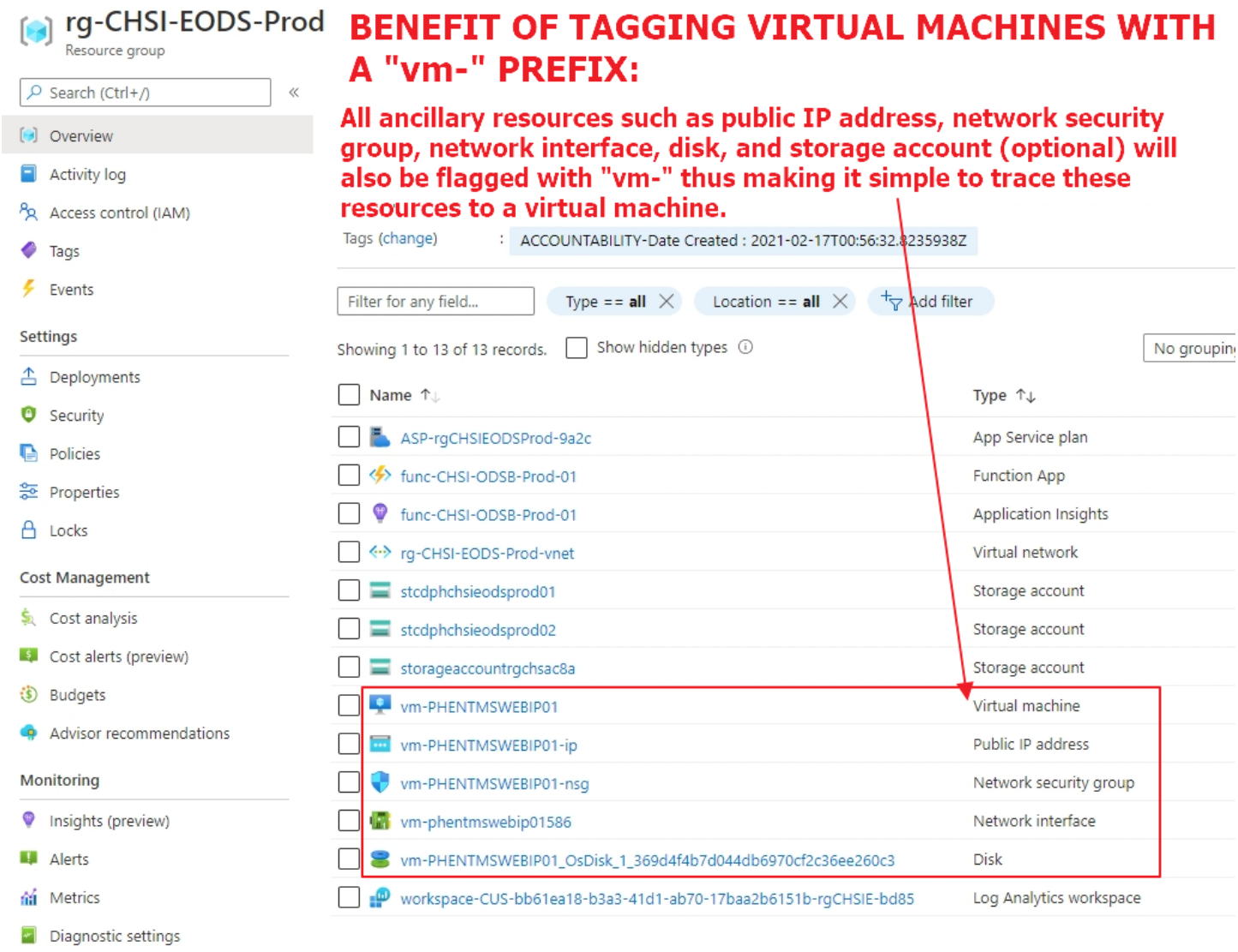


NetBIOS Active Directory Domain Name:



Naming Component	Description
Prefix	All virtual machines will begin with this prefix • (vm)
Public Health	CDPH servers
Owner	Business unit owner • (CHS) for CHSI • (ENT) for department-wide
Location	Server location • (TMS) for Tenant Managed Service (Rancho Cordova, CA) • (AZR) for Azure Cloud
Role	Server role • (APP) for application server • (WEB) for web server • (SQL) for SQL server
Environment	Server environment • (ID) for Development • (IS) for Staging • (IP) for Production
Instance	Server numerical instance

The benefit of a “vm-“prefix is evident in the screen shot below. In a list of resources, all Azure resources relating to the virtual machine “float” together as a cohesive unit.



NAMING CONVENTION: Entitlement Management Access Packages

An Azure AD Identity Governance feature, Entitlement Management removes barriers to internal and external collaboration by automating employee and partner access requests, approvals, auditing, and review. Entitlement Management provides administrators the ability to create, automate, and categorically group together necessary resources into what is called an access package.

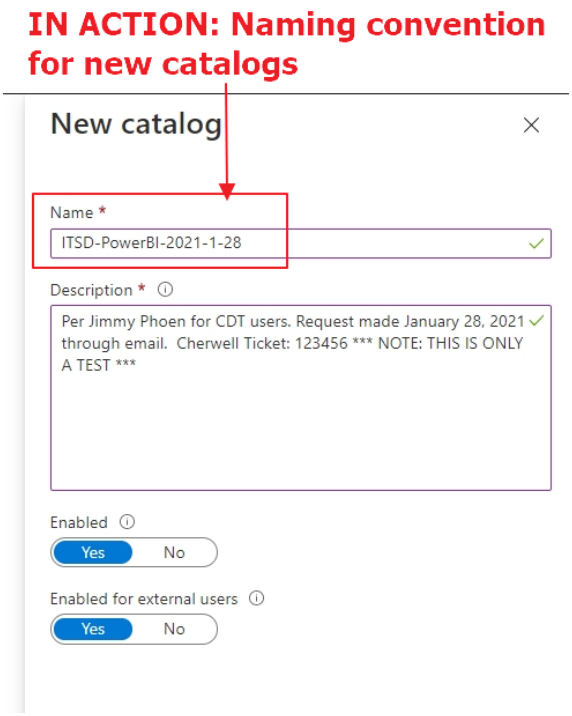
Access Package:

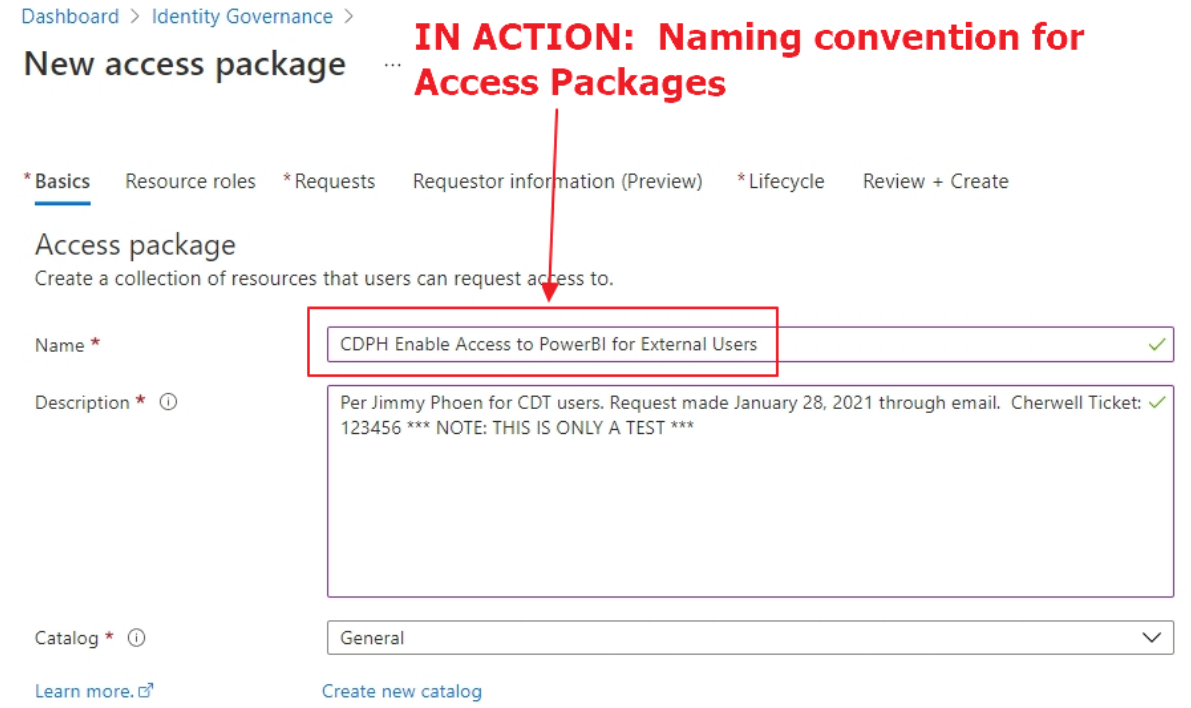
Access Package Catalog:

Naming Component	Description
Prefix	Prefix for all Access Packages created by CDPH. Note that a user may receive multiple access packages from various organizations in their My Access Portal. This prefix will readily identify a CDPH-originated access package and will facilitate easier identification. • (cdph)
Description	The description should include the Azure resource that is being provided to the end user as well as the nature of the end user (internal or external).
Business Unit Owner	The business unit which owns the access package catalog. Examples: • (ITSD) • (CHSI) • (ADSB) • (GDSP)

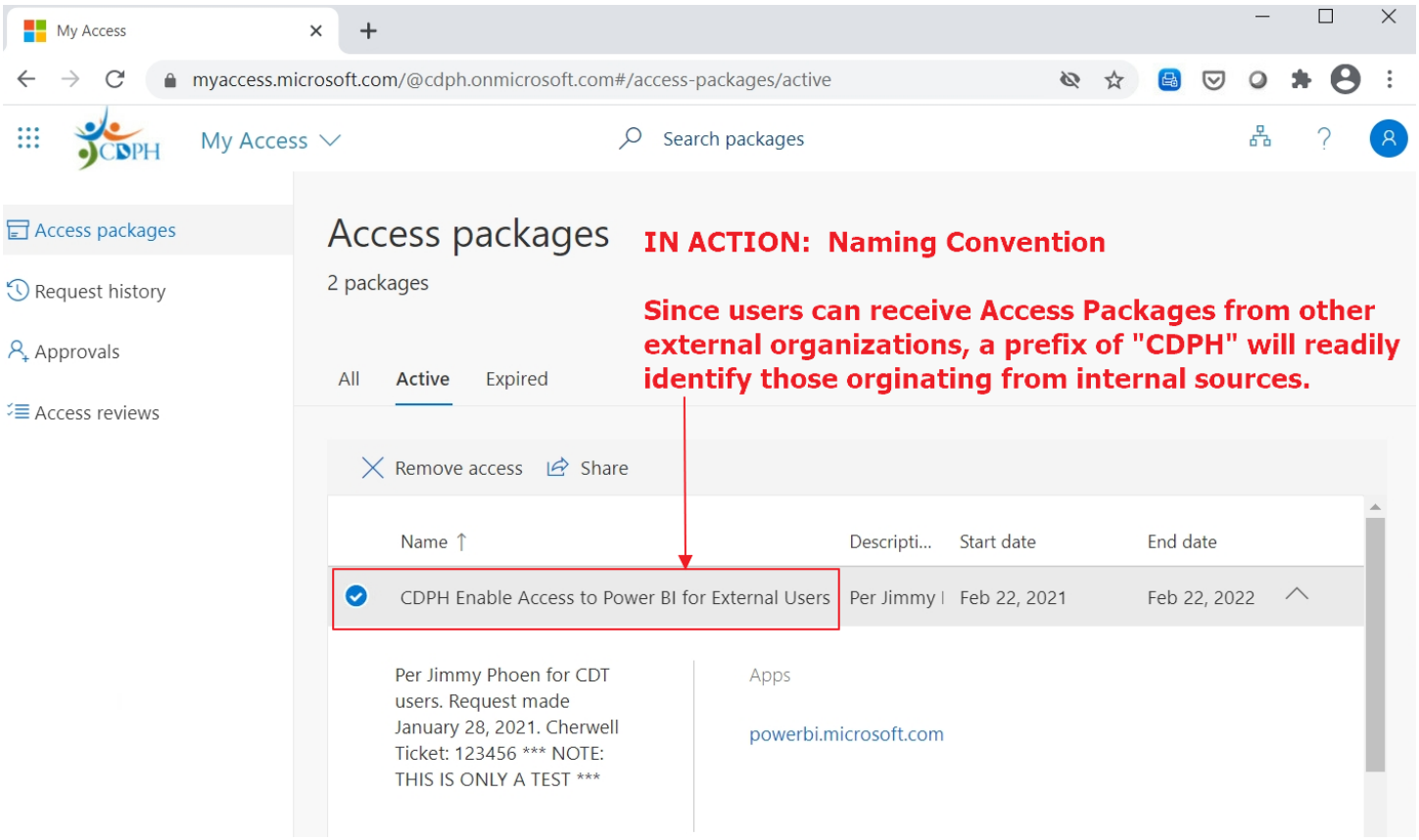
Resource	The specific Azure resource being delivered to the end user. Note that access packages deliver applications as well as group memberships. • Name of application • Name of AD security group for which the user is receiving membership.
Cherwell Change Control Date	Dates are extremely important for documentation purposes. For instance, given a date, one can search emails inboxes and Teams chats for further information on discussions revolving around the program or application or group membership in question. Here we are requesting the date of the Cherwell Change Control approval.

The series of screen shots below illustrate how the naming conventions are used in the creation of new Access Packages and Catalogs:





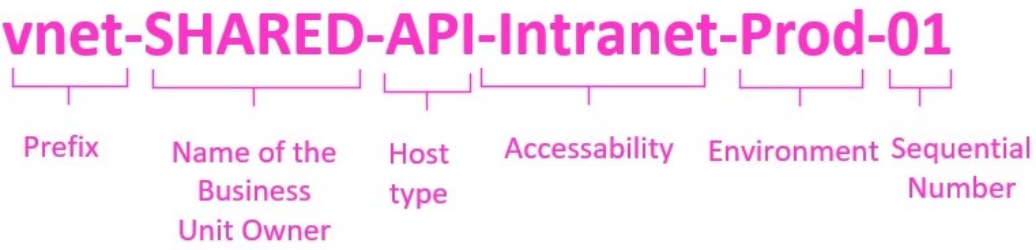
The screen shot below shows the My Access Portal, which is the way in which an end-user will be presented with an Access Package. Note that the end-user may receive access packages from other organizations with which CDPH has collaborative relationships. The prefix of "CDPH-"will allow the user to easily identify those Access Packages that originated from internal sources. This will also benefit external guest users (non-CDPH employees), as they will readily be able to identify those packages that originated from CDPH as opposed to other sources.



NAMING CONVENTION: Virtual Networks

An Azure virtual network is a fundamental building block for CDPH's private network in Azure. Virtual networks enable Azure resources to securely communicate.

Virtual Network Name:



Naming Component	Description
Prefix	All virtual networks will be prefixed with "vnet"
CDPH Business Unit Owner	The business unit which owns the virtual network. The example above shows "SHARED" which is shared by multiple business units.
Host type	The type of host that resides within the virtual network: • (APP) – An application is a standalone program • (API) – An API is a set of interfaces that perform very specific work.
Accessibility	Denotes the type of access this virtual network will have. • (Intranet) – Internal access only • (Extranet) – Accessible from the global internet • (Data) – Access to the backend database
Environment	• (Dev) – Development • (Stag) - Staging • (Prod) - Production
Sequence	Together with Environment, the numerical sequence Examples: • Prod-01 • Prod-02 • Prod-03…

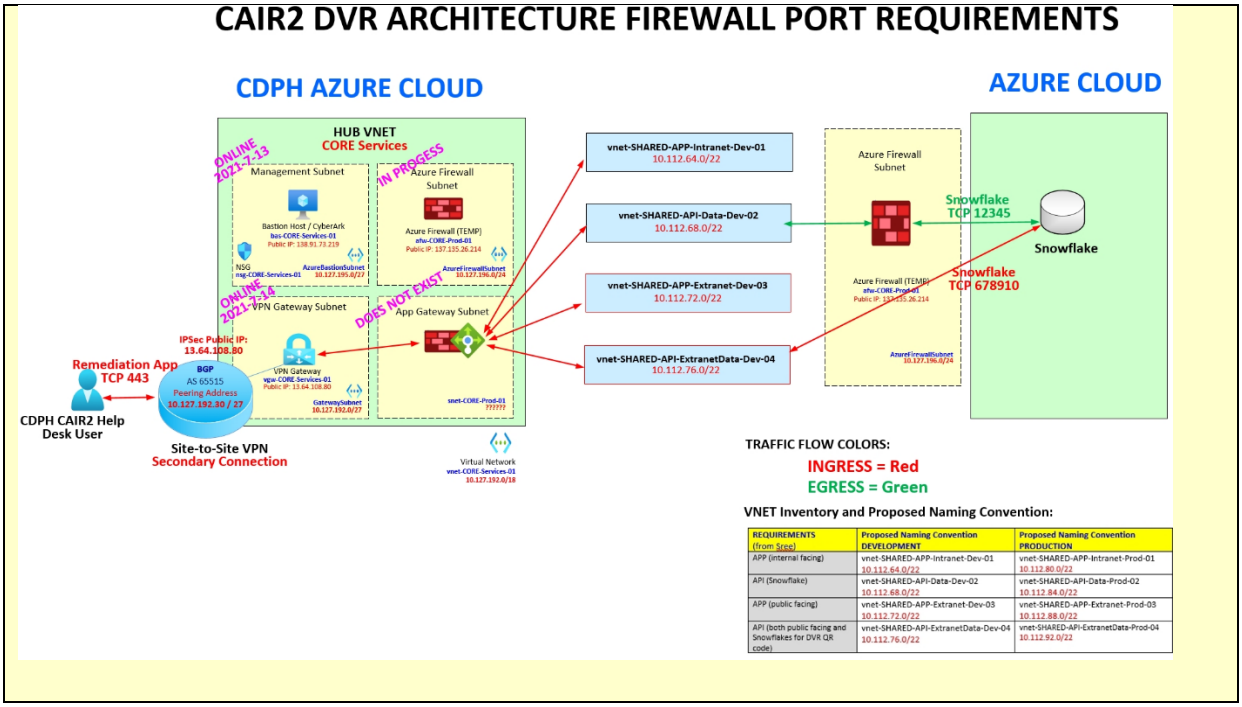
REFERENCE: VNet and subnet naming conventions are a result of collaborative effort with Sreekar Peddi of Tek Yantra during the development of CAIR2 DVR in July 2021:

From: Subido, James@CDPH
Sent: Friday, July 16, 2021 7:29 AM
To: Wu, Andy@CDPH <Andy.Wu@cdph.ca.gov>; Peddi, Sreekar@CDPH <Sreekar.Peddi@cdph.ca.gov>; Kanamaralapudi, Saiteja@CDPH <Saiteja.Kanamaralapudi@cdph.ca.gov>; Sadineni, Praveen@CDPH <Praveen.Sadineni@cdph.ca.gov>; Mathew, Swapna@CDPH <Swapna.Mathew@cdph.ca.gov>
Cc: Benson, Tyrone@CDPH <Tyrone.Benson@cdph.ca.gov>; Sanford, Ian@CDPH <Ian.Sanford@cdph.ca.gov>; Sheek, Wayne (CDPH-ITSD) <Wayne.Sheek@cdph.ca.gov>
Subject: REQUESTING FROM SREE: Firewall Port Requirements for CAIR2 DVR

Hello Sree,

Kindly document your firewall port requirements. I have documented a fictitious and completely fabricated port requirement for Snowflake and the Cair2 Help Desk user just to provide an example of what I'm looking for. I have attached the actual Visio file for you to edit.

The proposed naming convention for the VNets originated from both our established cloud governance standards and existing on-prem naming convention. To keep the Visio diagram simple, I have excluded the PROD VNets for now, assuming their port requirements will be the same as DEV. I will be off today but will be back on Monday to discuss during our meeting. Thanks, James



NAMING CONVENTION: Subnets

A subnet is a range of IP addresses within a virtual network. Subnets allow a virtual network to be subdivided into multiple subnets for organization and network security.

Subnet Name: snet-IB-CAIR2-DVRRemediationTool-API-Prod-01

Prefix	Name of the Business Unit Owner	Name of the Business Unit Program	Application Name	Host type	Environment	Sequential Number
snet	IB	CAIR2	DVRRemediationTool	API	Prod	01

Naming Component	Description
Prefix	All virtual networks subnets will be prefixed with “snet”
CDPH Business Unit Owner	The business unit which owns the subnet. The example shows “IB” which references the “Immunization Branch.
CDPH Business Unit Program	The specific business unit program hosted by the subnet.
Application Name	The specific application or workload hosted by the subnet.

Host type	The type of host that resides within the virtual network. Note, these host types are consistent with long-established CDPH N-Tier Architecture standards adopted for on-prem environments: • (USER)-Hosts that interact with the end user. • (APP) – An application is a standalone program • (API) – An API is a set of interfaces that perform very specific work. • (DATA)-Hosts that contain the data layer
Environment	• (Dev) – Development • (Stag) - Staging • (Prod) - Production
Sequence	Together with Environment, the numerical sequence Examples: • Prod-01 • Prod-02 • Prod-03…

NAMING CONVENTION: All Exception Resources such as Storage Accounts

Storage Accounts have the most restrictive naming requirements and, along with other Azure resources with severe restrictions such as Container Registries, fall into this category called "Exception Resources". Here are the restrictions for all "Exception Resources":

- 3 characters minimum and 24 characters maximum
- Lowercase and numbers only
- No dashes
- Globally unique

Storage Account Name: stcdphchsieodsprod01

- Prefix For Storage Accounts
- CDPH's Storage Accounts
- Business Unit
- Project
- Environment
- Instance

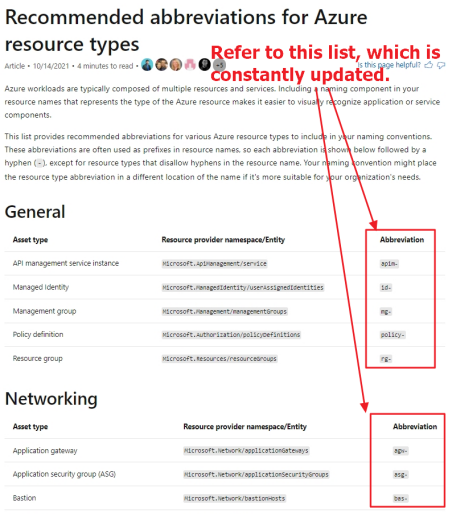
Naming Component	Description
Prefix	Prefix for storage accounts • (stcdph) Prefix for container registries

	• (crcdph)
Business Unit	The business unit which owns the storage account
Business Unit Program	The specific program or application associated with the storage account.
Environment	• Development (Dev) • Staging (Stag) • Production (Prod)
Instance	A numerical instance such as 01, 02, 03…

NAMING CONVENTION: All Other Resources

Azure provides an ever-growing list of hundreds of resources and services. For all other resources not explicitly mentioned in the previous section, the general naming convention below will apply. Here are examples of other resources and the use of the general naming convention:

Please refer to this list of recommended abbreviations to find the resource type that is not listed in this document.
[Recommended abbreviations for Azure resource types - Cloud Adoption Framework | Microsoft Docs]

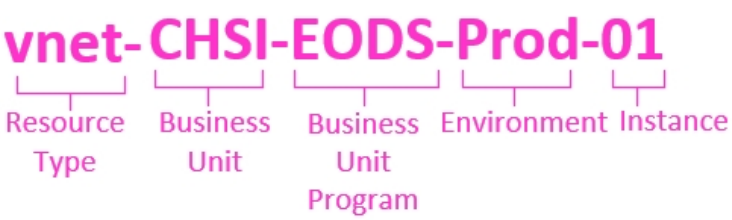


Log Analytics Workspace Name:

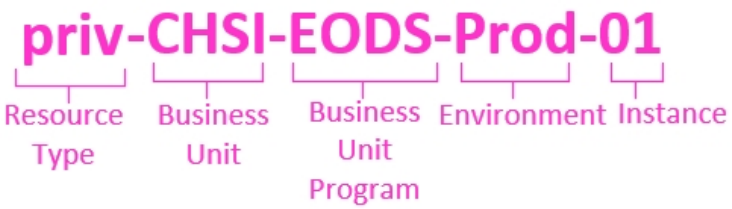
Key Vault Name:

Public IP Address Name:

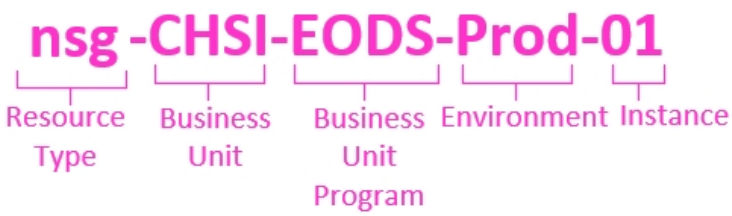
Virtual Network Name:

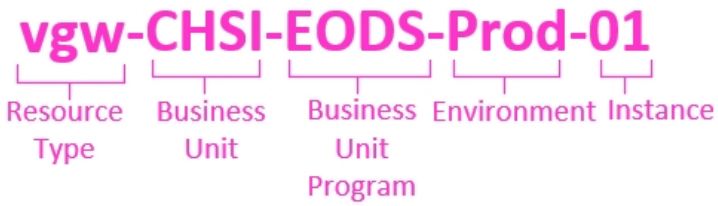


Private Endpoint Name:



Network Security Group Name:



Virtual Network Gateway: 

Naming Component	Description
Resource Type	The type of Azure Resource or Service. Examples: • (log) – Log Analytics Workspace • (rg) - Resource Group • (sa) - Storage Account • (dbs) - Databricks Service • (availt) - Availability Test
CDPH Business Unit	The business unit who owns the management group.
CDPH Business Unit Program	The specific program, application, or workload associated with the subscription.
Environment	• (Dev) - Development • (Stag) – Staging • (Prod) – Production
Instance	The sequential instance of the resource • (01) • (02) • (03) …

REFERENCES:

- Recommended Abbreviations for Azure Resources: Recommended abbreviations for Azure resource types - Cloud Adoption Framework | Microsoft Docs
- Azure Data Factory: Rules for naming Azure Data Factory entities - Azure Data Factory | Microsoft Docs

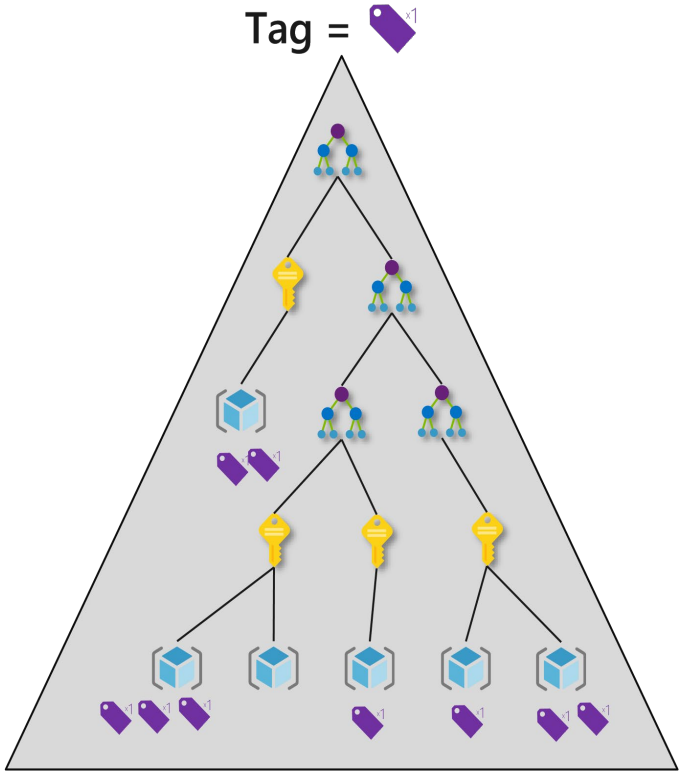
3. Resource Tags

Resource Tags in Azure provide CDPH with a means to apply additional metadata to Azure resources. This is a powerful feature that compliments the naming convention in the previous section.

Compared with naming conventions, Resource Tags are significantly more flexible and less structured. Another benefit to tags over names is that unlike Azure resource names which are static (most Azure resources are not easy to rename) resource tags can be changed at any time.

Benefits to resource tags:

- Manage complex collections of resources and resource groups
- Organize resources for billing and management
- Assign name-value pairs to Azure resources
- Define responsibility or ownership
- Enable consolidated billing views and analysis
- Attach metadata to resources through tags



Some important considerations:

- Each resource group or resource can have a maximum of 50 tags (as of April 2021).
- The tag name is limited to 512 characters. For storage accounts, this is limited even further to 128 characters.
- The tag value is limited to 256 characters
- Tags are not inherited for parent/child resources
- Some Azure resources cannot have tags (ex. generalized VM's, classic resources)
- The tag name prefixes "Azure," "Windows," and "Microsoft" are reserved and cannot be used

GOTCHA: Tags are not inherited from parent resource group. However, using Azure Policy, you can copy tags from parent resource group to the resource if a tag has not been populated.

Resource Tag Name: ACCOUNTABILITY-Owner (Category: ACCOUNTABILITY; Name: Owner)

Resource Tag Value: John Smith

Naming Component	Description
Category	To facilitate searching, Resource Tags are broken down into categories: • (ACCOUNTABILITY) • (SECURITY) • (LOCATION) IMPORTANT: Keep in mind that Resource Tags are flexible: you can add categories as required OR remove unused categories.
Name	The actual name of the Resource Tag.

CDPH RESOURCE TAGS:

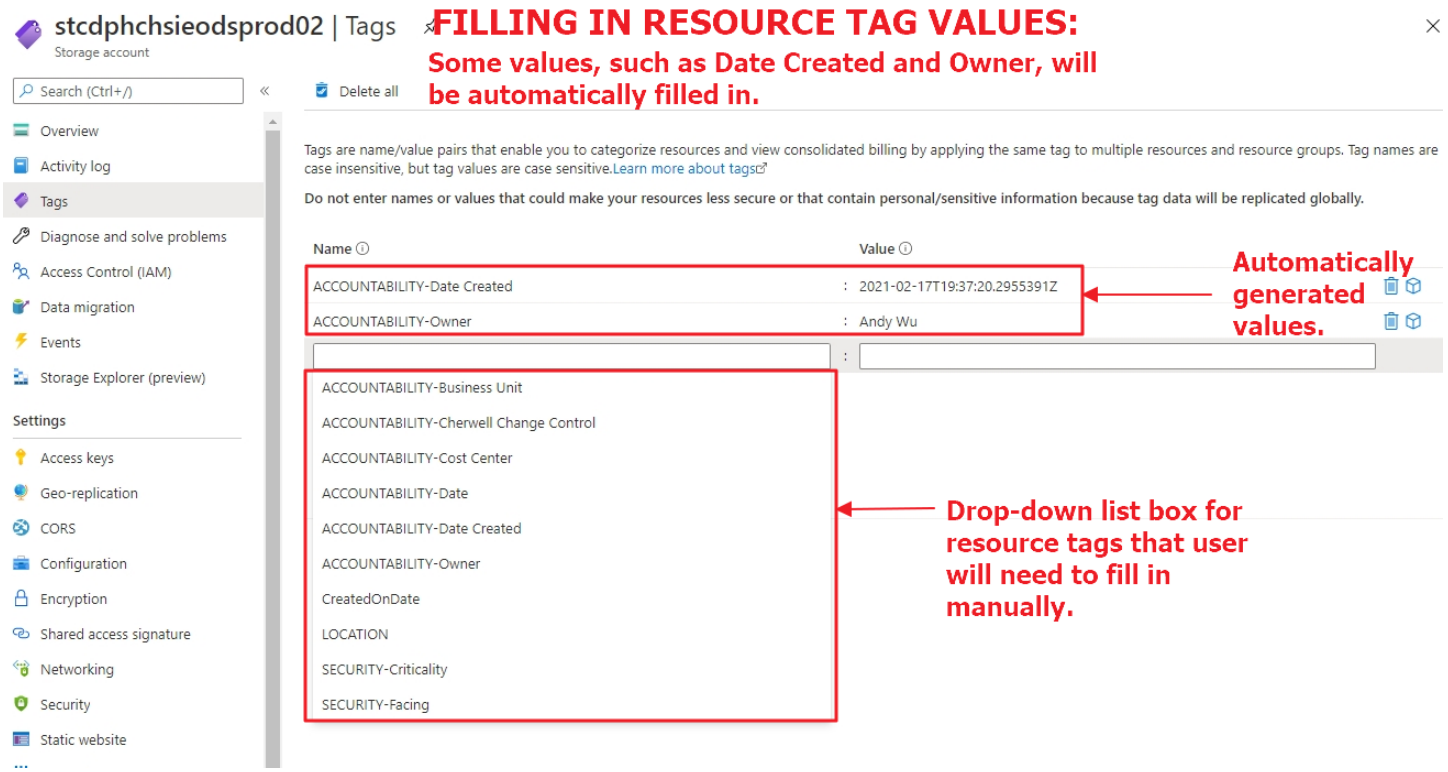
The following tags are currently with the goal of establishing them as a starting point to facilitate discussion:

Resource Tag Name	Description
ACCOUNTABILITY-Date Created	Date that the resource was created. (Automatic tag)
ACCOUNTABILITY-Owner	The name of the user who created the resource. (Automatic tag)
ACCOUNTABILITY-Business Unit	The business unit which owns the resource. (Automatic tag)
ACCOUNTABILITY-Program	The name of the program associated with the resource.
ACCOUNTABILITY-Cherwell Change Control	The approved Cherwell Change Control number.
ACCOUNTABILITY-Cost Center	Used for Cost Management (see Chapter 13)
ENVIRONMENT	Identify the resource as Test/Dev, Staging, or Production.
SECURITY-Criticality	Business impact in the event of an outage: High, medium, low
SECURITY-Facing	Is this resource accessible externally from the public cloud? Values available are: • Public Facing • Internal Facing

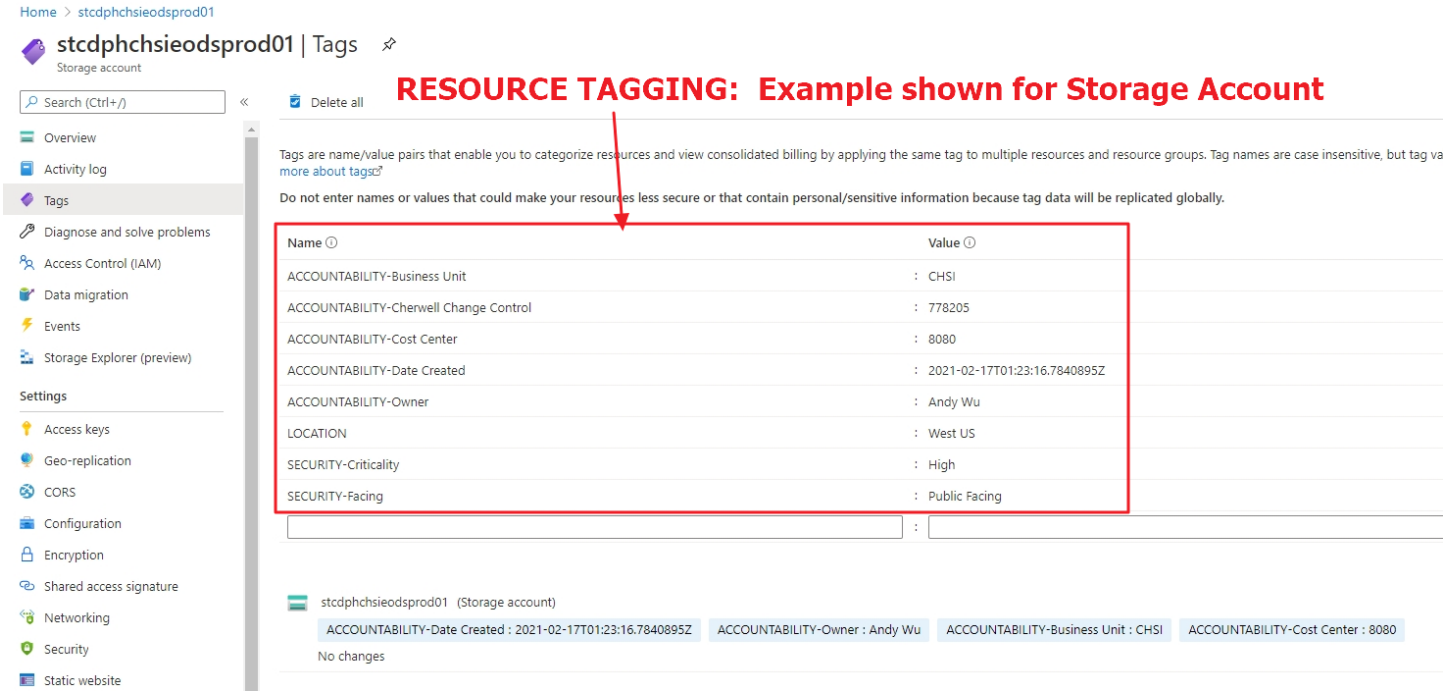
CDPH will implement Resource Tags in one of two ways:

1) Automatically filled tags are populated at time of creation without user intervention. Examples are “ACCOUNTABILITY-Owner” and “ACCOUNTABILITY-Creation Date” tags.

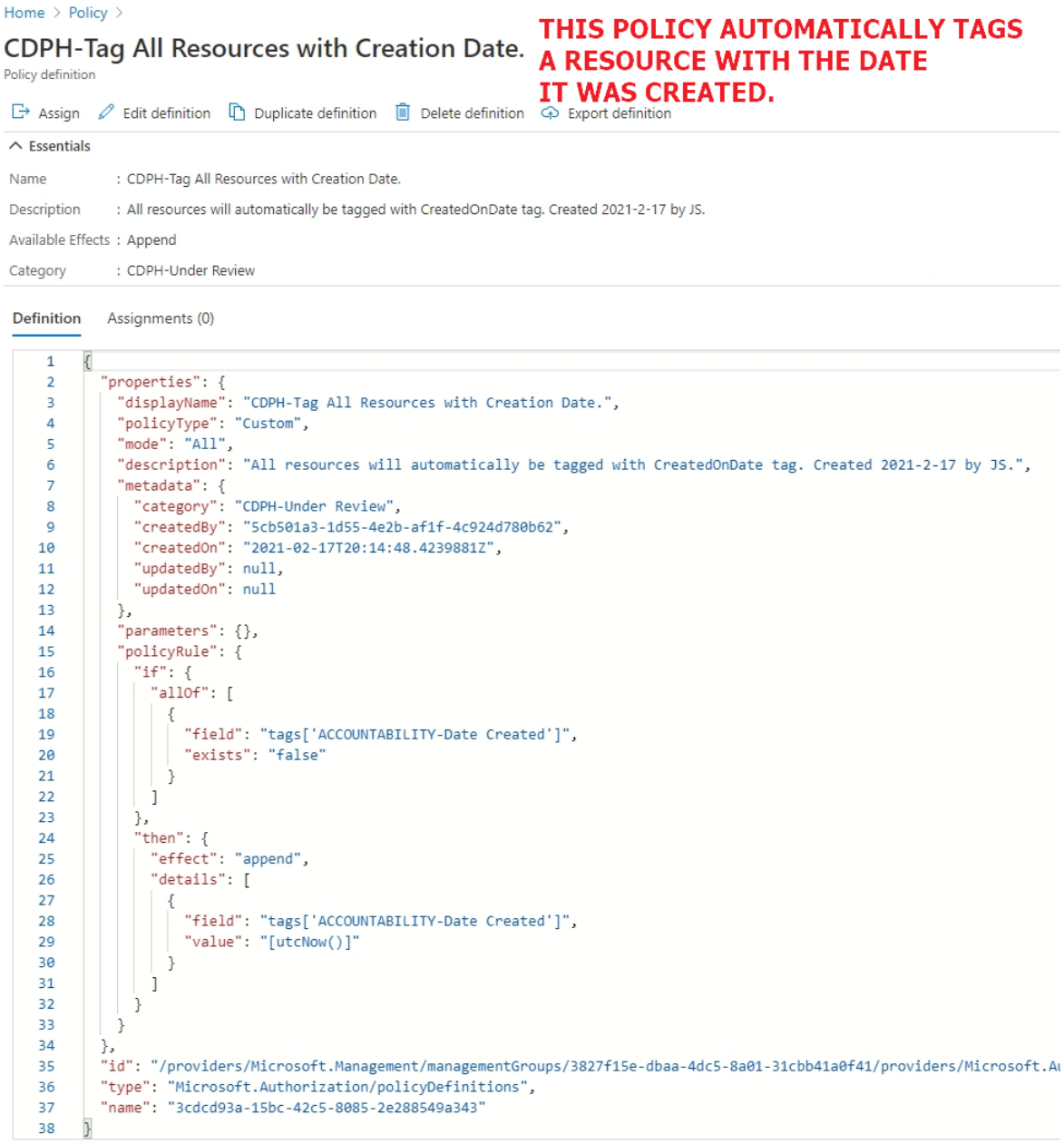
2) Manually filled tags which require user intervention.



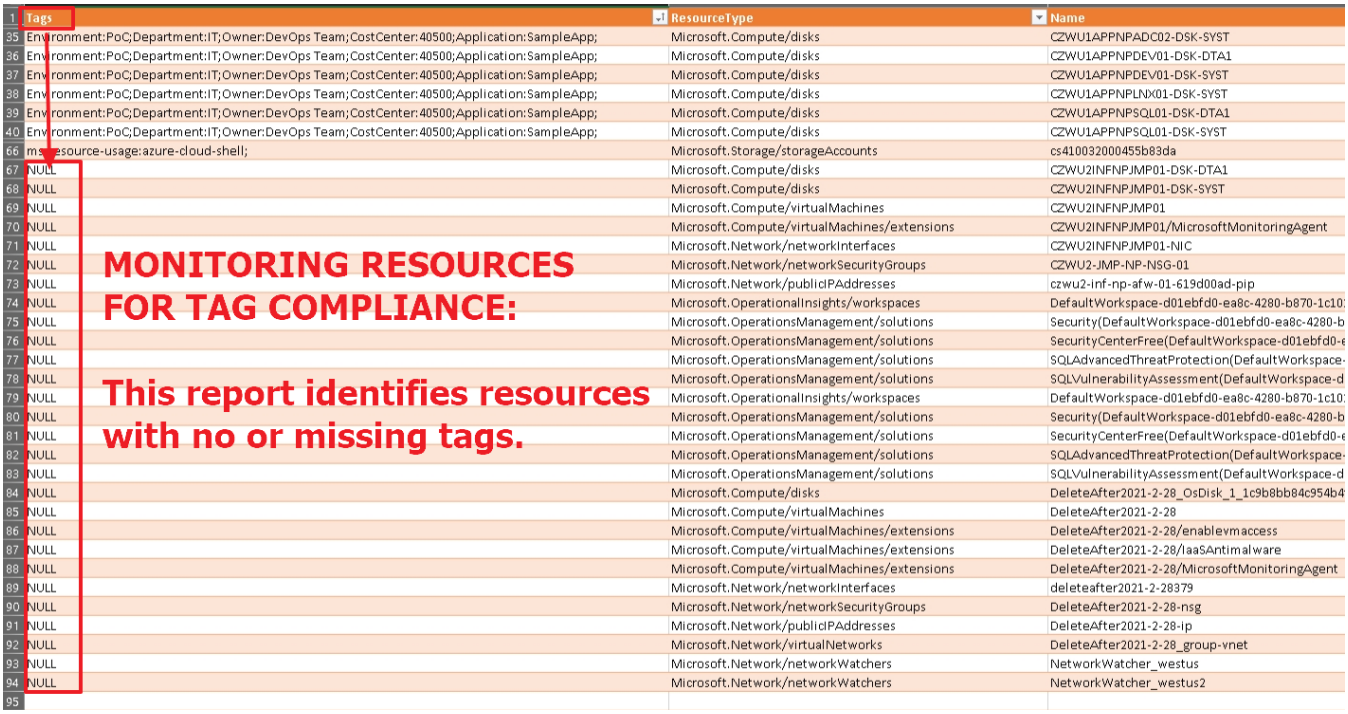
The screen shot below shows what Resource Tags look like with a sample resource in the form of a storage account.



To enforce Resource Tags that are automatically filled, we institute a policy such as “CDPH-Tag All Resources with Creation Date” below.



To monitor and verify for Resource Tag compliance, a PowerShell script or Resource Graph query can generate a CSV file which will identify resources that are missing tags such as that shown in the screen shot below:



	Tags	ResourceType	Name
35	Environment:PoC;Department:IT;Owner:DevOps Team;CostCenter:40500;Application:SampleApp;	Microsoft.Compute/disks	CZWU1APPNPADC02-DSK-SYST
36	Environment:PoC;Department:IT;Owner:DevOps Team;CostCenter:40500;Application:SampleApp;	Microsoft.Compute/disks	CZWU1APPNPDEV01-DSK-DTA1
37	Environment:PoC;Department:IT;Owner:DevOps Team;CostCenter:40500;Application:SampleApp;	Microsoft.Compute/disks	CZWU1APPNPDEV01-DSK-SYST
38	Environment:PoC;Department:IT;Owner:DevOps Team;CostCenter:40500;Application:SampleApp;	Microsoft.Compute/disks	CZWU1APPNPLNX01-DSK-SYST
39	Environment:PoC;Department:IT;Owner:DevOps Team;CostCenter:40500;Application:SampleApp;	Microsoft.Compute/disks	CZWU1APPNPSQL01-DSK-DTA1
40	Environment:PoC;Department:IT;Owner:DevOps Team;CostCenter:40500;Application:SampleApp;	Microsoft.Compute/disks	CZWU1APPNPSQL01-DSK-SYST
66	ms-resource-usage:azure-cloud-shell;	Microsoft.Storage/storageAccounts	cs410032000455b83da
67	NULL	Microsoft.Compute/disks	CZWU2INFNPJMP01-DSK-DTA1
68	NULL	Microsoft.Compute/disks	CZWU2INFNPJMP01-DSK-SYST
69	NULL	Microsoft.Compute/virtualMachines	CZWU2INFNPJMP01
70	NULL	Microsoft.Compute/virtualMachines/extensions	CZWU2INFNPJMP01/MicrosoftMonitoringAgent
71	NULL	Microsoft.Network/networkInterfaces	CZWU2INFNPJMP01-NIC
72	NULL	Microsoft.Network/networkSecurityGroups	CZWU2-JMP-NP-NSG-01
73	NULL	Microsoft.Network/publicIPAddresses	czwu2-inf-np-afw-01-619d00ad-pip
74	NULL	Microsoft.OperationalInsights/workspaces	DefaultWorkspace-d01ebfd0-ea8c-4280-b870-1c10
75	NULL	Microsoft.OperationsManagement/solutions	Security(DefaultWorkspace-d01ebfd0-ea8c-4280-b
76	NULL	Microsoft.OperationsManagement/solutions	SecurityCenterFree(DefaultWorkspace-d01ebfd0-e
77	NULL	Microsoft.OperationsManagement/solutions	SQLAdvancedThreatProtection(DefaultWorkspace-
78	NULL	Microsoft.OperationsManagement/solutions	SQLVulnerabilityAssessment(DefaultWorkspace-d
79	NULL	Microsoft.OperationalInsights/workspaces	DefaultWorkspace-d01ebfd0-ea8c-4280-b870-1c10
80	NULL	Microsoft.OperationsManagement/solutions	Security(DefaultWorkspace-d01ebfd0-ea8c-4280-b
81	NULL	Microsoft.OperationsManagement/solutions	SecurityCenterFree(DefaultWorkspace-d01ebfd0-e
82	NULL	Microsoft.OperationsManagement/solutions	SQLAdvancedThreatProtection(DefaultWorkspace-
83	NULL	Microsoft.OperationsManagement/solutions	SQLVulnerabilityAssessment(DefaultWorkspace-d
84	NULL	Microsoft.Compute/disks	DeleteAfter2021-2-28_OsDisk_1_1c9b8bb84c954b4
85	NULL	Microsoft.Compute/virtualMachines	DeleteAfter2021-2-28
86	NULL	Microsoft.Compute/virtualMachines/extensions	DeleteAfter2021-2-28/enablevmaccess
87	NULL	Microsoft.Compute/virtualMachines/extensions	DeleteAfter2021-2-28/IaaSAntimalware
88	NULL	Microsoft.Compute/virtualMachines/extensions	DeleteAfter2021-2-28/MicrosoftMonitoringAgent
89	NULL	Microsoft.Network/networkInterfaces	deleteafter2021-2-28379
90	NULL	Microsoft.Network/networkSecurityGroups	DeleteAfter2021-2-28-nsg
91	NULL	Microsoft.Network/publicIPAddresses	DeleteAfter2021-2-28-ip
92	NULL	Microsoft.Network/virtualNetworks	DeleteAfter2021-2-28_group-vnet
93	NULL	Microsoft.Network/networkWatchers	NetworkWatcher_westus
94	NULL	Microsoft.Network/networkWatchers	NetworkWatcher_westus2
95			

FOR DISCUSSION: Tagging is a powerful and flexible approach that gives CDPH the ability to add meaningful information to its resources. Unlike naming conventions which are difficult to change when requirements shift, tags can be created and deleted, as necessary. What are the other ways CDPH can leverage resource tagging? Would there be benefit in tagging shared resources for cost management purposes, for example?

4. Policies

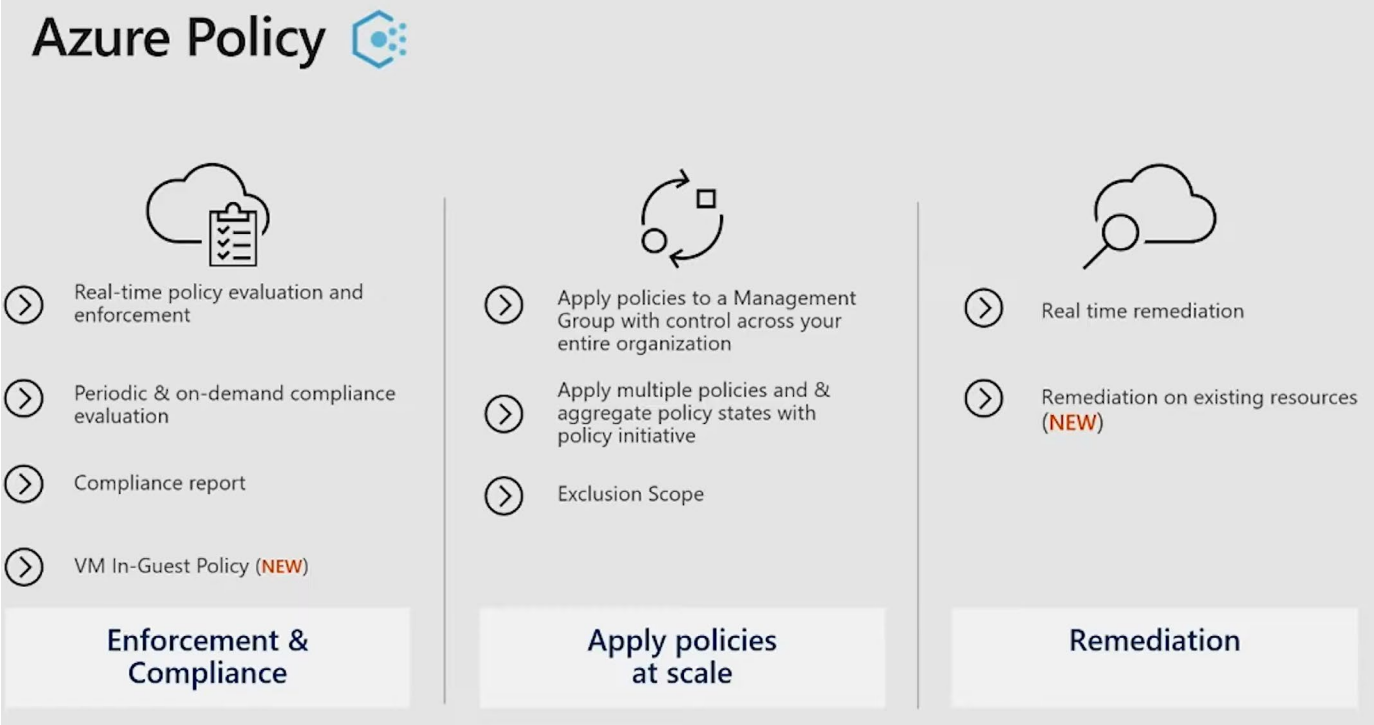
"Just because you can doesn't mean you should." – Mother

Azure Policy is a service that provides CDPH with the capability of enforcing its rules, standards, and controls to the resources it creates and manages in Azure. Policies provide the means to ensure the resources are compliant and remain compliant to the organizational guardrails throughout their life cycle; for example, they ensure that all resources are tagged with an owner and a creation date or that resources are only created in the West US region. CDPH can use Azure's pre-built policies or create its own.

Azure Policies are like Active Directory Group Policies in that they both flow down the resource hierarchy and the effective results are cumulative. While Group Policies have a "block inheritance"

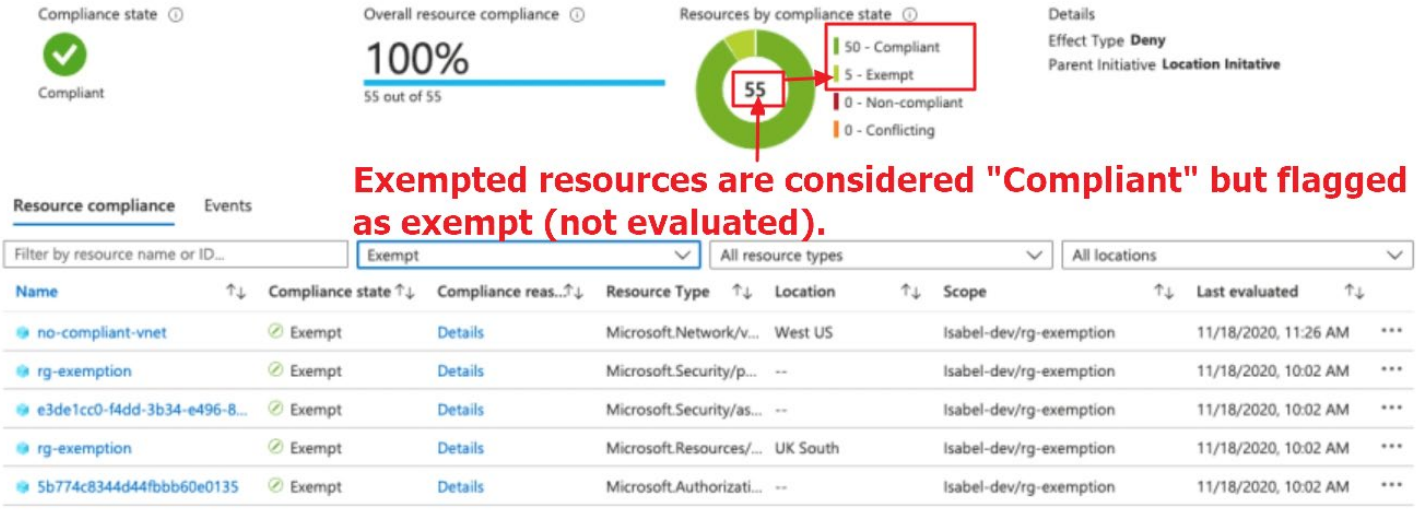
setting, Azure Policies have exclusions. However, they are different in that the order in which a given policy gets applied relative to others has no effect and the most restrictive policy will always win.

GOTCHA: Azure Policies are very different from Active Directory Group Policies in the area of precedence: The order in which a given policy is applied is irrelevant. All Azure policies are processed together and in the event of a conflict, the most restrictive policy will always win.



Policy Exemptions (Preview)

The Azure Policy exemptions (preview) feature is used to *exempt* a resource hierarchy or an individual resource from evaluation of initiatives or definitions. Resources that are *exempt* count toward overall compliance but cannot be evaluated or have a temporary waiver. The screen shot below illustrates this point:



You use JSON to create a policy exemption. The policy exemption contains elements for:

- display name
- description
- metadata
- policy assignment
- policy definitions within an initiative
- exemption category
- expiration

A policy exemption is created as a child object on the resource hierarchy or the individual resource granted the exemption. The target resource is not included in the exemption definition.

REFERENCE: [Details of the policy exemption structure - Azure Policy | Microsoft Docs]

Assigning Initiatives

Initiatives are collections of individual Azure policy definitions that are grouped together toward a specific goal or purpose in mind. Initiatives simplify the management of policies by grouping individual policies together as a collective single entity. The best practice is to deploy initiatives, not individual policies, for ease of management and maintenance.

Initiatives are assigned to either the management group, subscription, or resource group. The recommendation is to assign them to management groups, which are based on CDPH's business units (see *Chapter 6: Resource Hierarchy*). Unlike subscriptions and resource groups which are tied to a limited lifecycle, business units are persistent, making them suitable for initiative assignment. For those initiatives that require a global scope (they will need to apply across the board to all business units), the CDPH Root Management Group will serve as the assignment scope.

Policy Location

CDPH's custom policies and initiatives it creates require a storage location. The two options available to store policy and initiative definitions are a management group or a subscription. The location also determines where an initiative can be applied. As an example, a policy definition or initiative stored at a child management group level cannot be assigned to resources above the child management group or other child management groups at the same level. Once a definition location is selected and saved, it cannot be changed.

GOTCHA: Once a policy definition location is located and saved, it cannot be changed. The best practice recommendation is to save all policies and initiatives in the CDPH Root management group which will allow for both global and targeted deployment of policies throughout the entire resource hierarchy.

Policy Best Practices

1. Define Policies and Initiatives at the CDPH Root Management Group (as discussed above).
2. Before blocking users from working, test the Policy and Initiative by running them in audit mode, which will reveal the business impact that they will make prior to their enforcement.
3. Always create Initiative definitions even if they will only contain a single policy definition. With an initiative, you can always add new policies if needed.

Recommended Initiatives Using the MVP Approach

The Minimum Viable Product (MVP) approach highlights a lightweight starting point for governance. In other words, in order to achieve the highest likelihood of success with the least amount of risk and management pushback, CDPH will deploy, at first, the minimum number of policies when developing its governance framework for the first time.

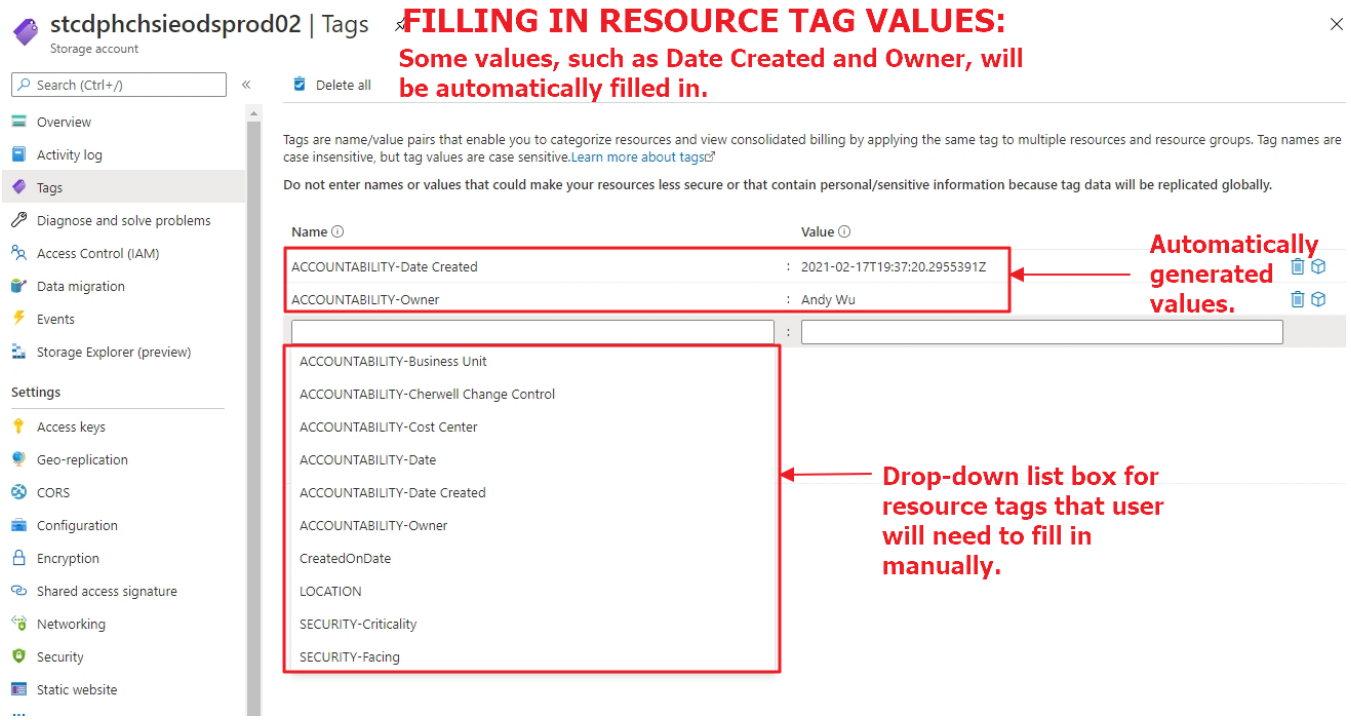
In keeping with the MVP approach, CDPH will be deploying two initiatives: 1) CDPH Baseline and 2) HIPAA/HITRUST Regulatory Compliance.

INITIATIVE #1: CDPH Baseline Initiative

The goal of the CDPH Baseline Initiative is to address existing concerns and issues on hand. Here are a few policies:

POLICY: CDPH-Tag resource with Owner Name and Date

Tag all resources with the name of the owner who created the resource and the date of creation. This makes auditing easier as it will provide the answer to *"Who created what and when?"*



FOR DISCUSSION: CDPH has the option of enforcing Cherwell Change Control number when an Azure admin creates a new resource. The name of the resource tag is "ACCOUNTABILITY-Cherwell Change Control" as shown in the list box above.

POLICY: CDPH-Restrict all Resources to West US Region (Not West US2)

The general best practice is to select an Azure region that is closest to the physical location of most of its users OR farthest away if the requirement is data redundancy. Since disaster recovery is out of scope for this document, the recommendation is to store all Azure resources in the West US region (San Francisco). The map below shows the exact location of West US and West US2:

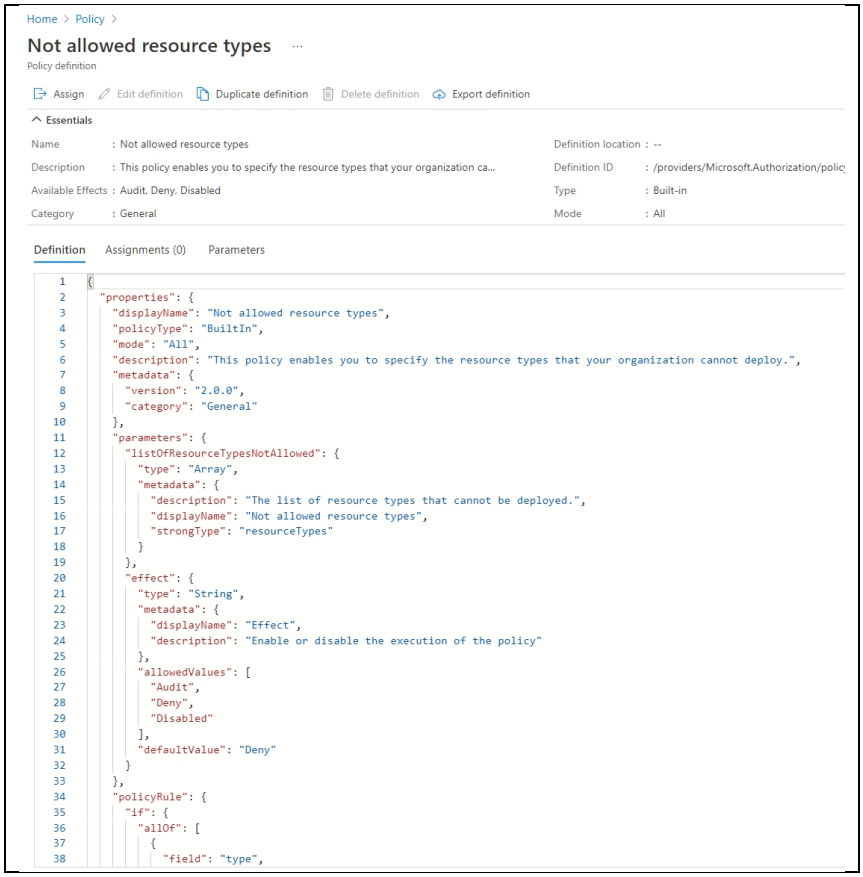
FOR DISCUSSION: The recommendation of West US is in line with the general recommendation of interoperability with an on-prem datacenter in Sacramento and the location of most of CDPH's users. However, West US2 has the following two advantages: 1) Lower cost; 2) Azure Availability Zones are currently (March 2021) not supported in West US.

POLICY UPDATE: Aa of June 17, 2021: USWest2 is CDPH's REGION

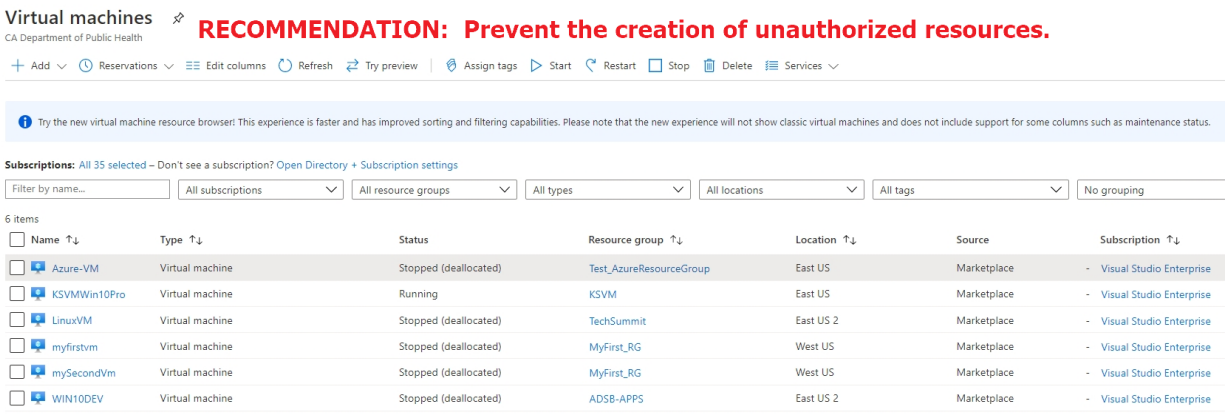
The Governance Team, in an effort to take advantage of new Azure features that will be released to USWest2 ahead of USWest, has decided to standardize on the creation of all Azure Resources to USWest2.

POLICY: CDPH-Not Allowed Resource Types

One of the foundations of governance is *"Just because you can doesn't mean you should"*. This policy will block the deployment of specific Azure resources. The "Not Allowed Resources Types" is a built-in policy that will require customization using a JSON editor such as Microsoft Visual Studio Code.



The following screen shot below shows unauthorized virtual machines being created.



Here is a list of the individual policies (three of which were discussed above) that comprise the CDPH Baseline Initiative:

Individual Policies for CDPH Baseline Initiative

1. Restrict all resources to WestUS region
2. Deny resource types
3. Tagging (ACCOUNTABILITY-Owner) applied to resource groups.
4. Tagging (ACCOUNTABILITY-Creation Date) applied to resource groups.
5. Tagging (ACCOUNTABILITY-Business Unit) applied to resource groups.
6. Tagging (ACCOUNTABILITY-Cost Center) applied to resource groups.
7. Tagging (ACCOUNTABILITY-Cherwell Ticket) user prompted -- applied to resource groups.
8. Allowed Storage Account SKUs (choose while deploying)
9. Allowed Azure VM SKUs (choose while deploying)
10. Require Network Watcher to be deployed
11. Require Azure Storage Account Secure Transfer Encryption

INITIATIVE #2: CDPH HITRUST/HIPAA

Governments and regulatory organizations frequently publish standards to help define good security practices so that organizations can avoid negligence. The purpose and scope of these standards and regulations vary, but the security requirements can influence the design for data protection and retention, data privacy, and system security.

Details of the HIPAA HITRUST 9.2 Regulatory Compliance built-in initiative

02/09/2021 • 96 minutes to read •

The following article details how the Azure Policy Regulatory Compliance built-in initiative definition maps to **compliance domains** and **controls** in HIPAA HITRUST 9.2. For more information about this compliance standard, see HIPAA HITRUST 9.2. To understand *Ownership*, see Azure Policy policy definition and Shared responsibility in the cloud.

The following mappings are to the **HIPAA HITRUST 9.2** controls. Use the navigation on the right to jump directly to a specific **compliance domain**. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **HITRUST/HIPAA** Regulatory Compliance built-in initiative definition.

This built-in initiative is deployed as part of the HIPAA HITRUST 9.2 blueprint sample.

Important

Each control below is associated with one or more **Azure Policy** definitions. These policies may help you **assess compliance** with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time. To view the change history, see the **GitHub Commit History**.

REFERENCE: Regulatory Compliance details for HIPAA HITRUST 9.2 - Azure Policy | Microsoft Docs

The HIPAA HITRUST initiative Is a built-in initiative comprised of the following individual policies:

FOR DISCUSION: The 50 policies below come with the built-in Azure HITRUST/HIPAA Initiative. A determination will need to be conducted on each policy as to whether it would be appropriate for CDPH's environment.

Individual Policies for HIPAA HITRUST Initiative

1 [Preview]: Container Registry should use a virtual network service endpoint
2 A maximum of 3 owners should be designated for your subscription
3 A vulnerability assessment solution should be enabled on your virtual machines
4 An activity log alert should exist for specific Administrative operations
5 Audit diagnostic setting
6 Audit usage of custom RBAC rules
7 Audit Windows machines missing any of specified members in the Administrators group
8 Audit Windows machines on which the Log Analytics agent is not connected as expected
9 Audit Windows machines that have extra accounts in the Administrators group
10 Azure Key Vault Managed HSM should have purge protection enabled
11 CORS should not allow every resource to access your Web Applications
12 Cosmos DB should use a virtual network service endpoint
13 Deprecated accounts with owner permissions should be removed from your subscription
14 Diagnostic logs in App Services should be enabled
15 Diagnostic logs in Azure Stream Analytics should be enabled
16 Diagnostic logs in Data Lake Analytics should be enabled
17 Diagnostic logs in Key Vault should be enabled
18 Diagnostic logs in Service Bus should be enabled
19 Enforce SSL connection should be enabled for MySQL database servers
20 Enforce SSL connection should be enabled for PostgreSQL database servers
21 Ensure WEB app has 'Client Certificates (Incoming client certificates)' set to 'On'
22 Event Hub should use a virtual network service endpoint
23 External accounts with owner permissions should be removed from your subscription
24 Function App should only be accessible over HTTPS
25 Geo-redundant backup should be enabled for Azure Database for MySQL
26 Geo-redundant backup should be enabled for Azure Database for PostgreSQL
27 Internet-facing virtual machines should be protected with network security groups
28 Key Vault should use a virtual network service endpoint
29 Latest TLS version should be used in your API App
30 Latest TLS version should be used in your Function App
31 Latest TLS version should be used in your Web App
32 Long-term geo-redundant backup should be enabled for Azure SQL Databases
33 MFA should be enabled on accounts with read permissions on your subscription
34 Microsoft Antimalware for Azure should be configured to automatically update protection signatures
35 Monitor missing Endpoint Protection in Azure Security Center
36 Network Watcher should be enabled

37 Resource logs in Azure Key Vault Managed HSM should be enabled
38 SQL Server should use a virtual network service endpoint
39 Storage Accounts should use a virtual network service endpoint
40 Subnets should be associated with a Network Security Group
41 The Log Analytics agent should be installed on Virtual Machine Scale Sets
42 The Log Analytics agent should be installed on virtual machines
43 Virtual machines should be connected to an approved virtual network
44 Vulnerabilities in container security configurations should be remediated
45 Vulnerabilities in security configuration on your machines should be remediated
46 Vulnerabilities on your SQL databases should be remediated
47 Vulnerability assessment should be enabled on your SQL servers
48 Web Application should only be accessible over HTTPS
49 Windows machines should meet requirements for 'Security Options - User Account Control'
50 Windows machines should meet requirements for 'User Rights Assignment'

5. Role Based Access Control (RBAC)

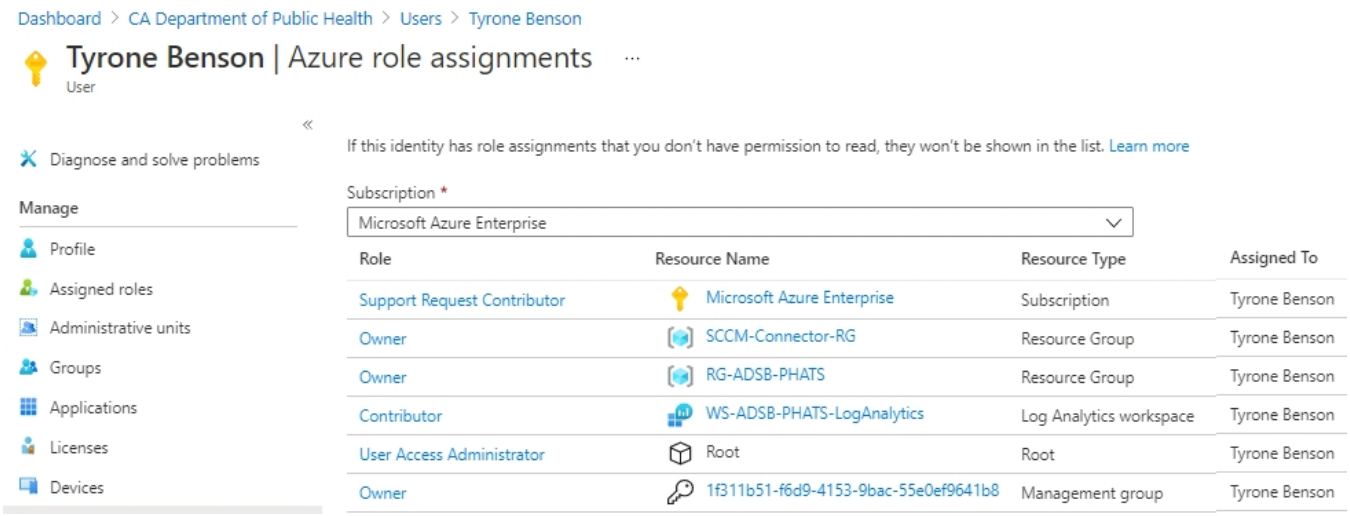
"Technology makes it possible for people to gain control over everything, except technology." – John Tudor

Role-based access control (RBAC) is a component of the governance framework for organizations. RBAC ensures that only authorized and approved users have appropriate access to resources. In Azure, RBAC has predefined roles that you can use to grant access at the management group, subscription, resource group, or resource level.

Azure provides over 120 built-in RBAC roles. Some of the commonly used built-in roles which apply for all resources (not specific to a resource provider) are shown in the screen shot below:

Built-in role	Description
General	
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Reader	View all resources, but does not allow you to make any changes.
User Access Administrator	Lets you manage user access to Azure resources.

Here is a screen shot of RBAC assignments for a particular user:



Custom roles are available to extend and adjust the default role permissions to suit specific requirements of CDPH. A recommended practice is to create and deploy custom roles only when built-in roles are not adequate. Also consider assigning several built-in roles instead of creating a unique custom role.

Custom Roles

RECOMMENDATION: Create Custom Roles only when built-in roles do not meet requirements.

Custom roles can be created if the built-in roles do not meet requirements	Easiest way to create is using an existing role as the foundation exported to JSON	Specific actions for types of resource from resource providers can be configured

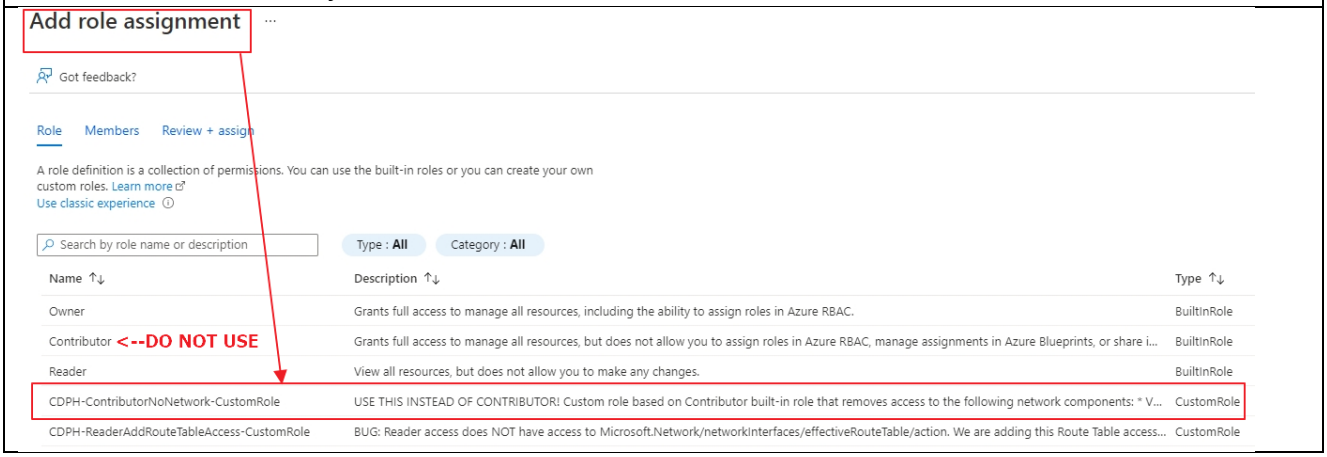
GOTCHA: Custom RBAC roles may present more risk and surely generate more validation work since a custom role that works today may not continue to work in the future due to the dynamic world of Azure. Use built-in roles whenever possible.

UPDATE: December 15, 2021: Replacement of Contributor Built-In Role

USE THIS INSTEAD OF CONTRIBUTOR! Azure's built in Contributor role delegates too many privileges. Instead of using Contributor, use the custom role called "CDPH-ContributorNoNetwork-CustomRole". It is based on the Contributor built-in role but removes access to the following network components:

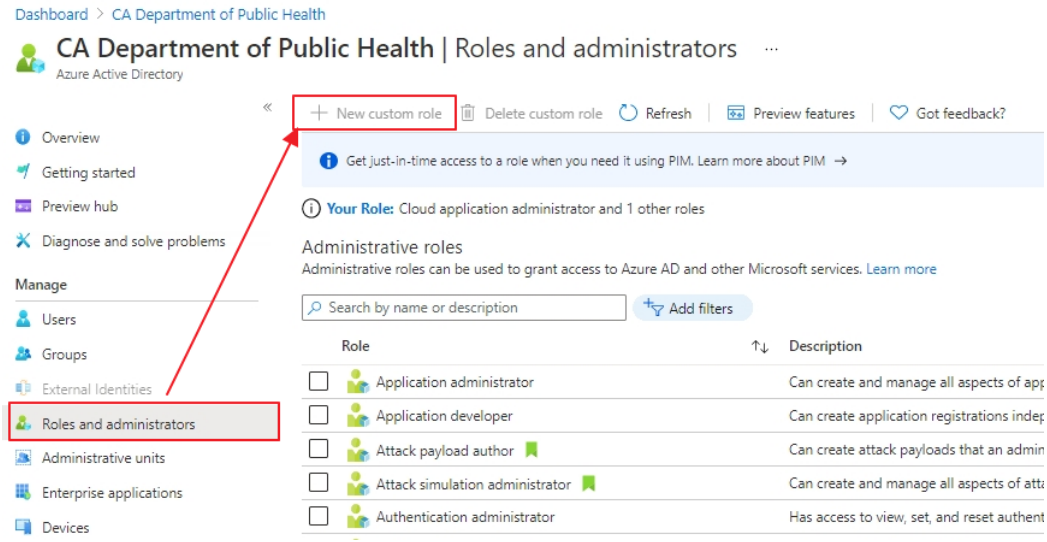
- VNets and Subnets
- Network Security Groups
- Route Tables

Created 2021-10-21 by James Subido



Note that there are two different types of custom RBAC roles:

- **Custom Azure AD RBAC roles** which are created from the Azure portal as shown here:



- **Custom RBAC roles for Azure resources** are created using PowerShell, CLI, or REST API. The screen shot below is an example of a custom role definition for a role called "*Virtual Machine Operator*". This custom role is required for those environments where "*Virtual Machine Contributor*" provides excessive permissions while "*Virtual Machine Administrator Login*" does not provide enough. Key to this custom role is the ability to start and restart

virtual machines as seen in the "Actions" section below:

Create VM Operator role definition

JSON

```
{
"Name": "Virtual Machine Operator",
"Id": "88888888-8888-8888-8888-888888888888",
"IsCustom": true,
"Description": "Can monitor and restart virtual machines.",
"Actions": [
  "Microsoft.Storage/*/read",
  "Microsoft.Network/*/read",
  "Microsoft.Compute/*/read",
  "Microsoft.Compute/virtualMachines/start/action",
  "Microsoft.Compute/virtualMachines/restart/action",
  "Microsoft.Authorization/*/read",
  "Microsoft.ResourceHealth/availabilityStatuses/read",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Insights/alertRules/*",
  "Microsoft.Support/*"
],
"NotActions": [],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
   "/subscriptions/{subscriptionId1}"
]
}
```

The above JSON file is saved as "vm-operator-role.json" and the following PowerShell is executed to create the new custom role:

Azure CLI

```
az role definition create --role-definition vm-operator-role.json
```

REFERENCE: [What are custom roles in Azure? - Learn | Microsoft Docs]

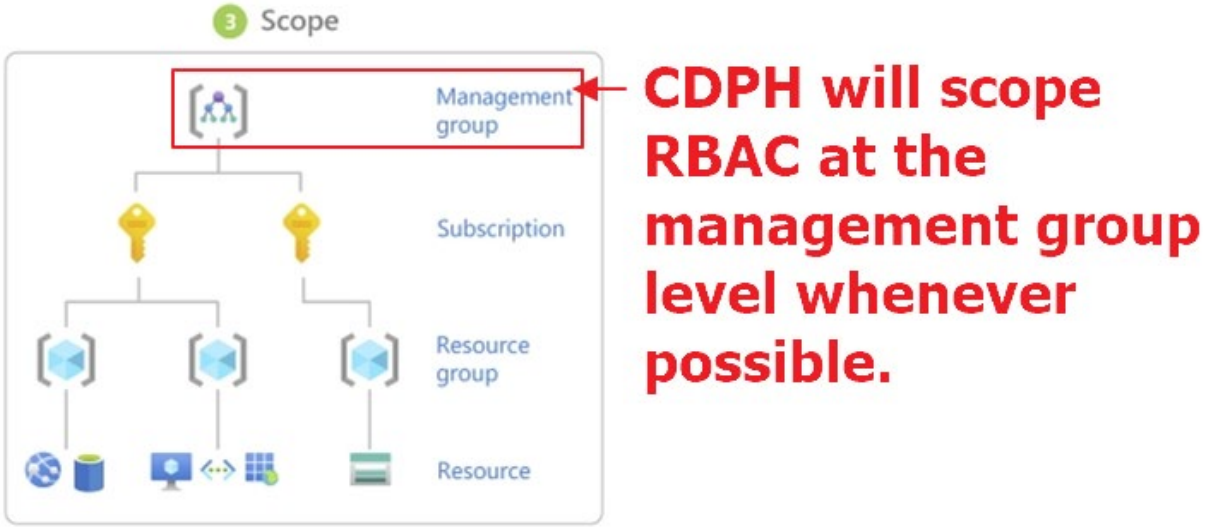
RBAC's Three Key Elements

An RBAC role assignment has three key elements:

1. A **security principal**, which can be either one of users, groups, or service principals.

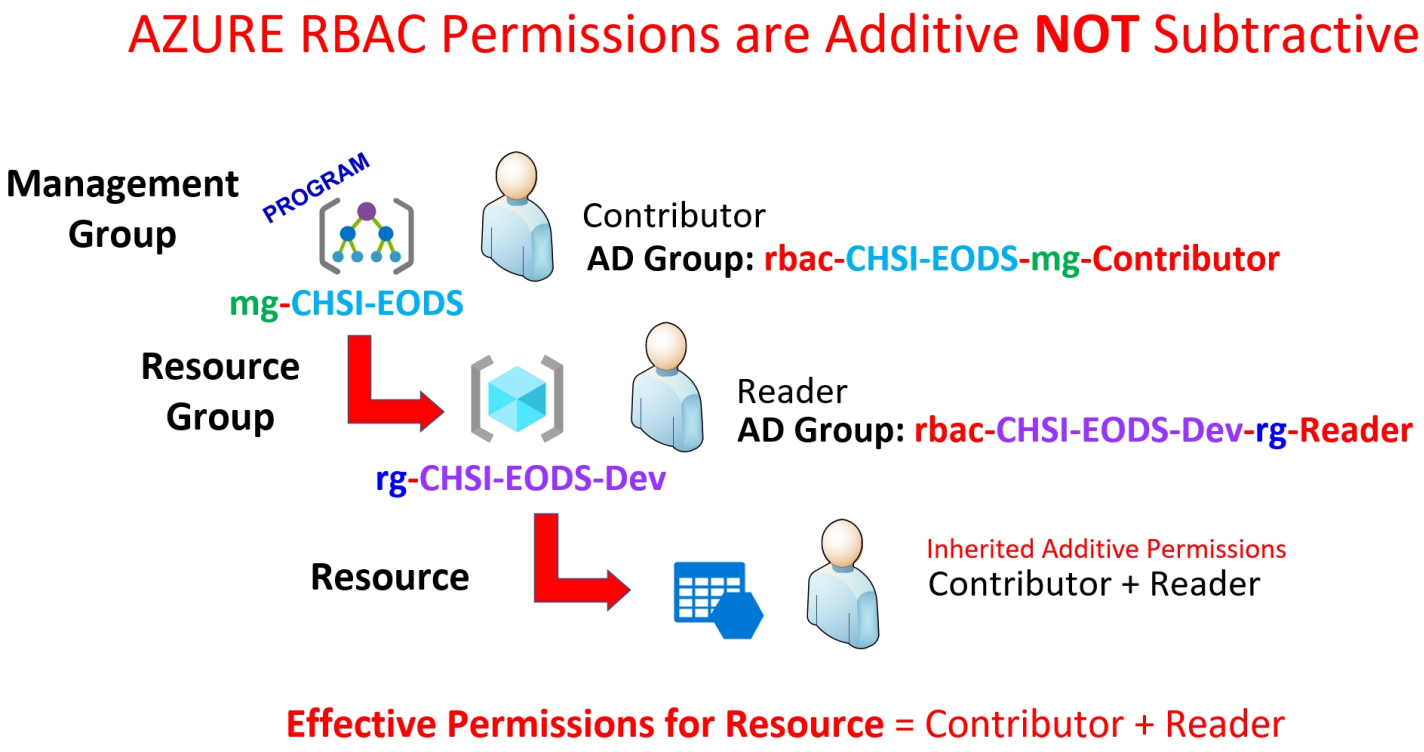
2. A **role**, which describes a set of management permissions. For example, the contributor role contains all actions, except authorization-related rights. Consequently, a contributor may manage all aspects at a given scope without being able to grant access to resources for other users.

3. A **scope** to set the access rights, starting from the management group level down to single resources.



RBAC is a cumulative allow model. When you are assigned a role, RBAC allows you to perform certain actions, such as read, write, or delete. For instance, if one role assignment grants you read permissions to a management group and a different role assignment grants you write permissions to the same management group, your effective permissions will be read and write.

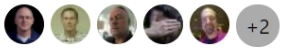
The screen shot below illustrates the cumulative allow model in action. Note that the better approach in this situation is to give the user Reader permissions at the Management Group level and Contributor level at the Resource Group Level. In other words start with more restrictive permissions at the top of the hierarchy.



RBAC role assignments are cumulative unless there is a deny assignment, which is used to block a user from performing specific Azure resource actions even if a role assignment grants them access. Deny assignments are typically used when a built-in RBAC role grants too many privileges which will require a deny assignment to revoke them.

Keep in mind that Azure has a limit of 2,000 role assignments per subscription. The recommended work around is to use groups instead of individual user accounts for RBAC role assignments, which is consistent with recommended best practice. The screen shot below provides additional detail on this:

Troubleshoot Azure RBAC

04/06/2021 • 12 minutes to read • 

This article answers some common questions about Azure role-based access control (Azure RBAC), so that you know what to expect when using the roles and can troubleshoot access problems.

Azure role assignments limit

Azure supports up to **2000** role assignments per subscription. This limit includes role assignments at the subscription, resource group, and resource scopes. If you get the error message "No more role assignments can be created (code: RoleAssignmentLimitExceeded)" when you try to assign a role, try to reduce the number of role assignments in the subscription.

> ⓘ Note **As of April 2021, Azure has a limit of 2,000 role assignments per subscripton.**
>
> The **2000** role assignments limit per subscription is fixed and cannot be increased.

If you are getting close to this limit, here are some ways that you can reduce the number of role assignments: **Use groups instead of individual accounts.**

- Add users to groups and assign roles to the groups instead.
- Combine multiple built-in roles with a custom role.
- Make common role assignments at a higher scope, such as subscription or management group.
- If you have Azure AD Premium P2, make role assignments eligible in Azure AD Privileged Identity Management instead of permanently assigned.
- Add an additional subscription.

REFERENCE: Troubleshoot Azure RBAC | Microsoft Docs

GOTCHA: As of March 2021, you cannot directly create your own deny assignments. Azure Blueprints (covered in Chapter 14) and Azure managed apps are the only way that deny assignments can be created.

REFERENCE: Understand Azure deny assignments - Azure RBAC | Microsoft Docs

The next section will go over the critical importance of using AD Groups as security principals for assigning RBAC.

The Key to Successful and Efficient RBAC: Azure AD Groups

While we can assign RBAC roles and privileges to individual user accounts directly, this practice becomes very hard to manage in the long term as it is not easy to audit and over time, users end up with access to every single object in Azure because these role assignments are never revoked. Instead, best practice dictates the use of AD groups to assign RBAC roles and privileges. Additionally, in most organizations including CDPH, very few requirements are unique to a person. We generally have roles within the department that perform certain functions. We gather these functions as a collective group when they have common requirements. Fulfilling these requirements as a group assigned through RBAC is efficient and effective.

Azure AD Groups	• Avoid assigning privileges, roles, and access to individual user accounts as this is very difficult to manage. • Instead, we add users to groups and assign RBAC to groups • Groups can replicate from AD the same way as users • Groups can be assigned access, roles, and licenses.

By simply adding or removing a user from a given AD group, that user inherits RBAC roles and privileges. This practice is already in place for CDPH's on-prem AD in terms of granting users access to file systems, servers, and SCCM-provided applications. In August 2020, Microsoft Azure released this capability as a public preview as shown in the screen shot below:

Alex Simons (AZURE) Microsoft 08-13-2020 01:00 PM

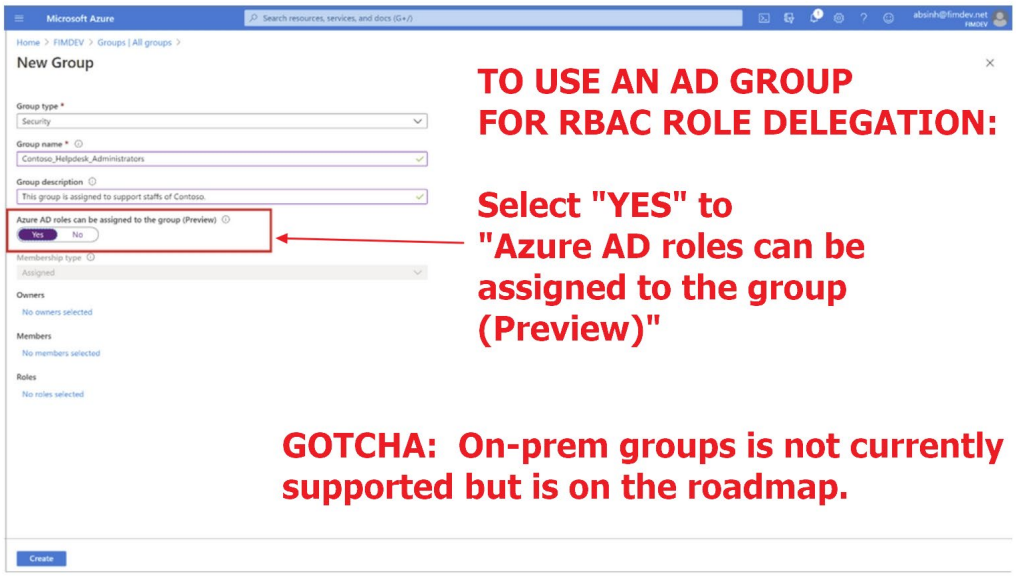
PUBLIC PREVIEW: August 2020

Assigning groups to Azure AD roles is now in public preview!

Howdy folks,

Today, we're excited to share that you can assign groups to Azure Active Directory (Azure AD) roles, now in public preview. Role delegation to groups is one of the most requested features in our feedback forum. Currently this is available for Azure AD groups and Azure AD built-in roles, and we'll be extending this in the future to on-premises groups as well as Azure AD custom roles.

To use this feature, you'll need to create an Azure AD group and enable it to have roles assigned. This can be done by anyone who is either a Privileged Role Administrator or a Global Administrator.

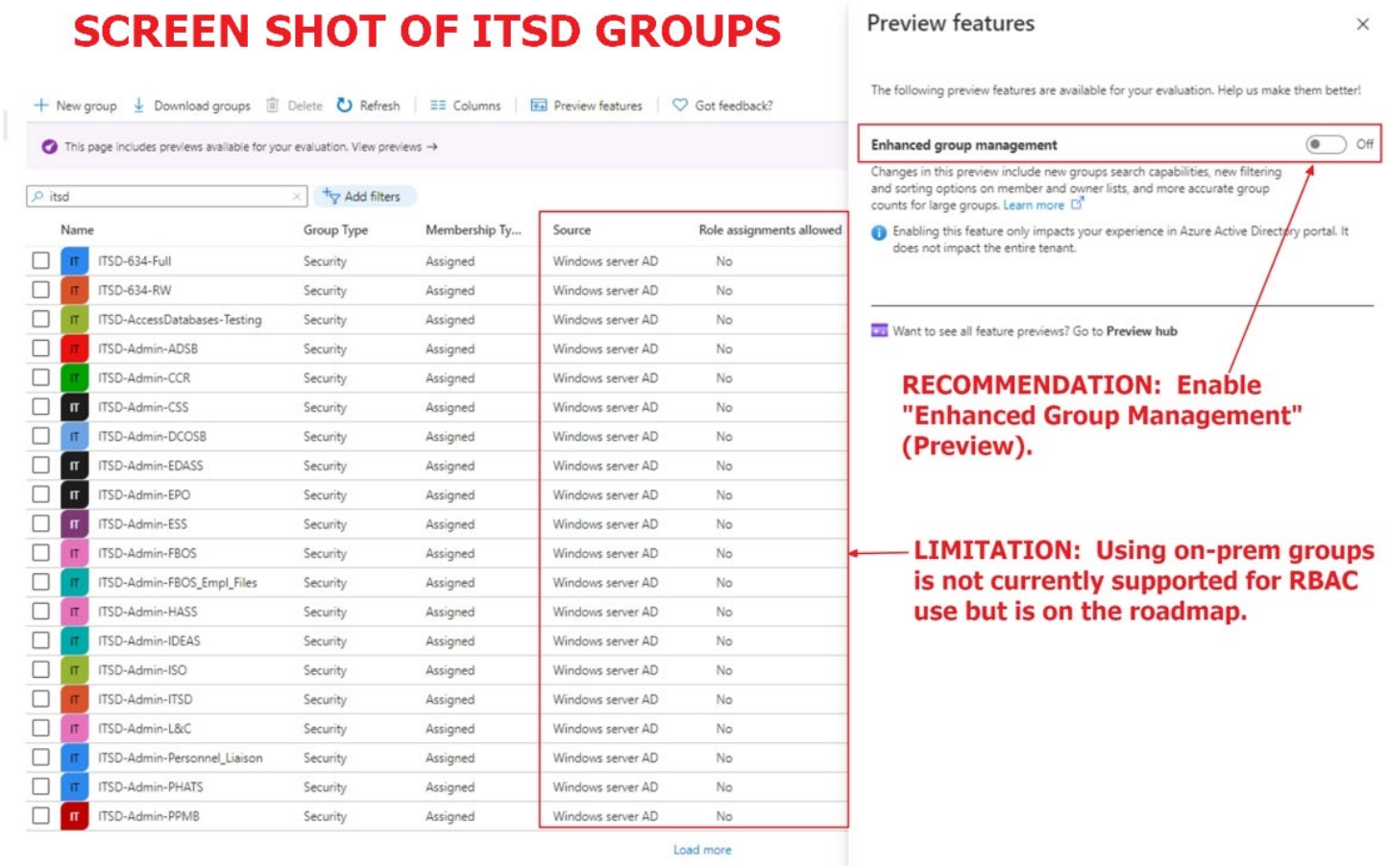


After that, any of the Azure AD built-in roles, such as Teams Administrator or SharePoint Administrator, can have groups assigned to them.

REFERENCE: Assigning groups to Azure AD roles is now in public preview! - Microsoft Tech Community

FOR DISCUSSION: On-prem AD groups cannot be used for RBAC role assignments; however, this is on the roadmap and will be supported in the future (timeline uncertain). Will CDPH use cloud AD groups in the interim?

The screen shot below shows the limitation of on-prem AD groups' lack of RBAC role assignment capability. However, Microsoft has expressed this as already in their roadmap for future support (timeline unknown).



A recommendation is to use “Enhanced Group Management”, which enables group search, filtering and sorting options, and accurate group counts.

Search groups and members (preview) in Azure Active Directory

12/02/2020 • 3 minutes to read • **PUBLIC PREVIEW: December 2020**

This article tells you how to search for members and owners of a group and how to use search filters as part of the groups improvement preview in the Azure Active Directory (Azure AD) portal. There are lots of improvements in the groups experiences to help you manage your groups, including members and owners, quickly and easily. For more information about previews, see Supplemental Terms of Use for Microsoft Azure Previews.

Changes in this preview include:

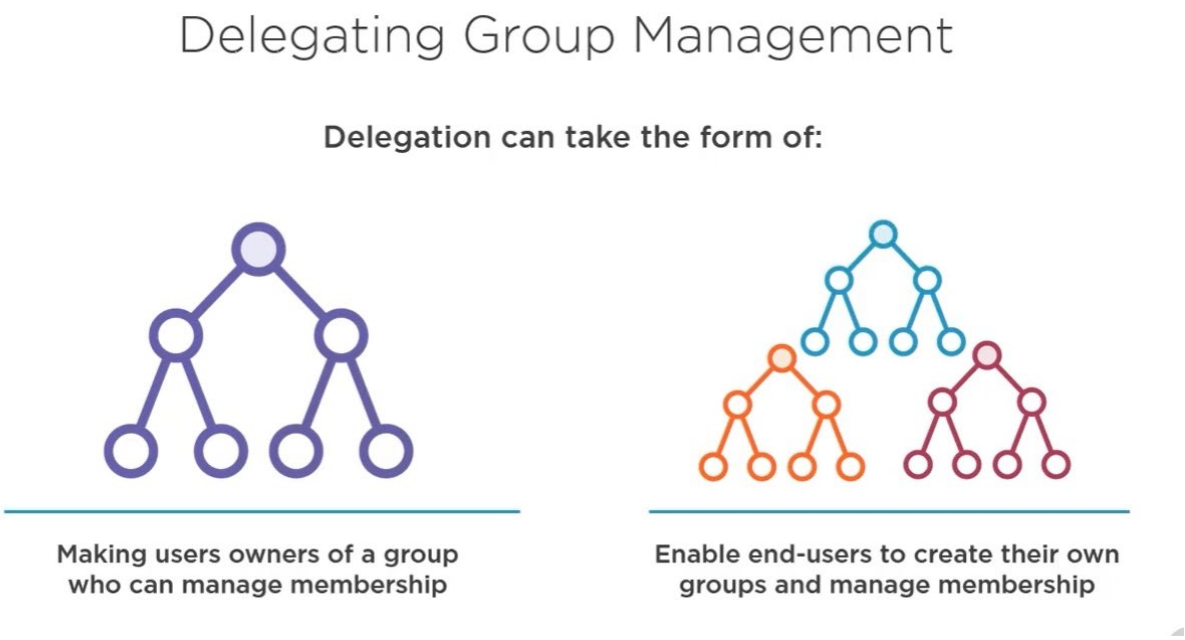
- New groups search capabilities, such as substring search in group names
- New filtering and sorting options on member and owner lists
- New search capabilities for member and owner lists
- More accurate group counts for large groups

Remember that while identifying the minimum rights required to perform the role is always more work than assigning the user with higher, more generic permissions, the increased security gained is well worth the effort.

The Key to Successful and Efficient RBAC: Group Management through the Access Panel

Business unit managers are best suited to managing group members as they really understand who members of a given group should be, the business context for their membership, and the lifecycle of the membership. (Best practice dictates that membership to a group should ideally be associated with a limited lifecycle or lifespan). We can make business unit managers (who are not Azure AD admins) the owners of their own group and manage the memberships themselves.

By empowering business unit managers with the day-to-day control of group membership, CDPH may reap benefits in the form of reduced Help Desk calls and increased security through Access Reviews (also conducted by the business unit manager).

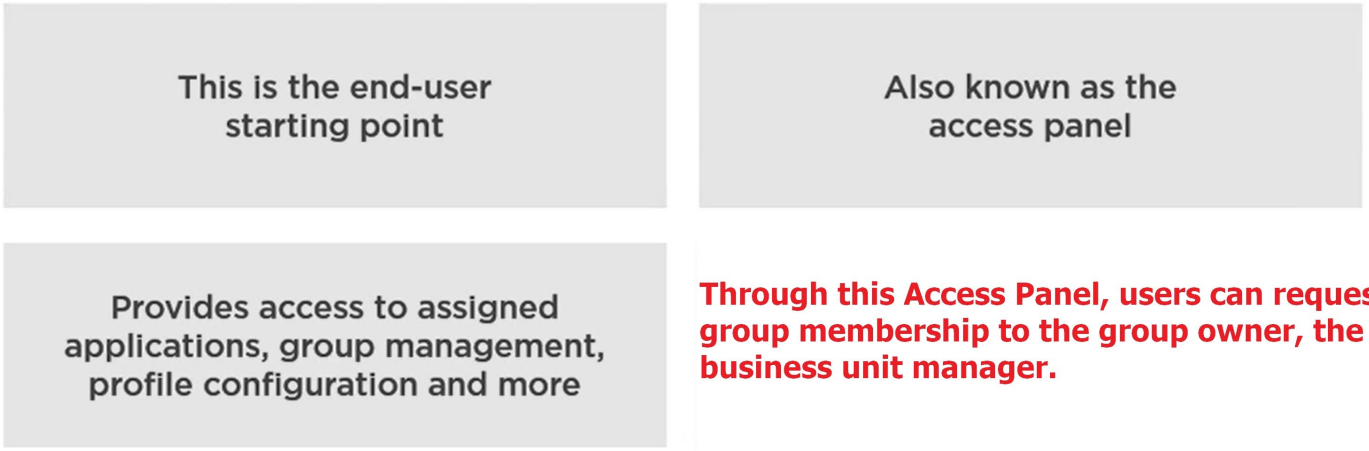


The Access Panel (also known as My Apps portal (myapps.microsoft.com) is a web-based portal for managing and launching apps, self-manage groups, and execute self-service password resets. The portal is available to all users by default and cannot be turned off. Microsoft recommends configuring My Apps portal for the best possible end-user experience.

myapplications.microsoft.com

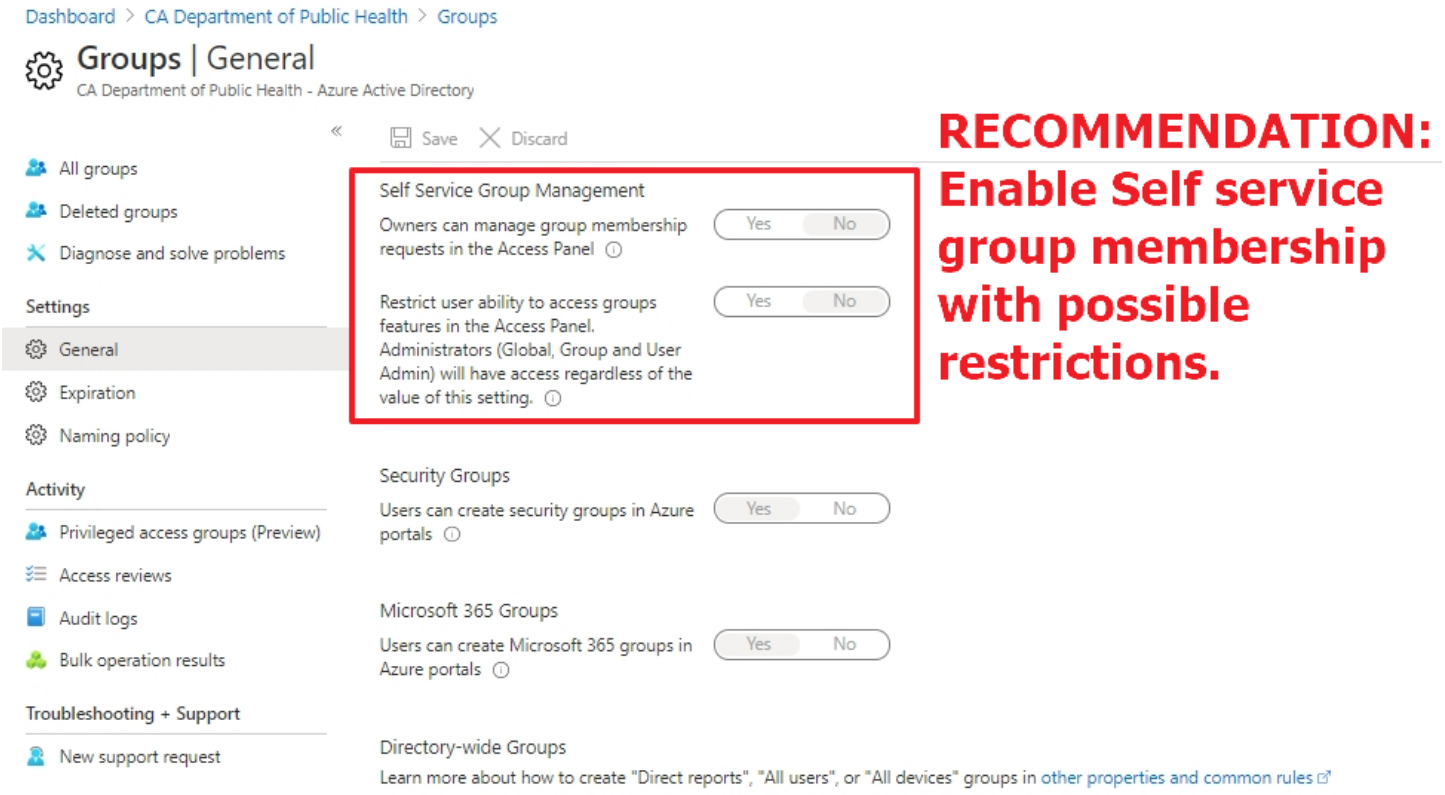
also accessible as "myapps.microsoft.com"

Delegating Group Membership to Business Unit Managers



IMPORTANT NOTE: CDPH business unit managers will not be allowed the ability to create security groups. That process will be left to Azure administrators due to its implications with RBAC.

The screen shot below provides the recommended changes to **Groups -> General to** enable self-service group membership. Self-service group management enables users to manage their own security groups (or Microsoft 365 groups) in Azure AD. The owner of the group (the CDPH business unit manager), can approve or deny the requests.



First, we have that **Owners can manage group membership requests in the Access Panel**. If a user requests to be a member of a group, owners will have the ability to approve or deny that request. The recommended setting is to enable self-service group management by selecting "Yes".

The second is **Restrict access to Groups in the Access Panel.** This option determines whether in the Access Panel users will be able to see other groups and try to join them. CDPH would want to restrict users from being able to see other groups that either 1) do not apply to them or 2) are not authorized to join. The recommended setting for this is to enable the restriction by selecting "Yes".

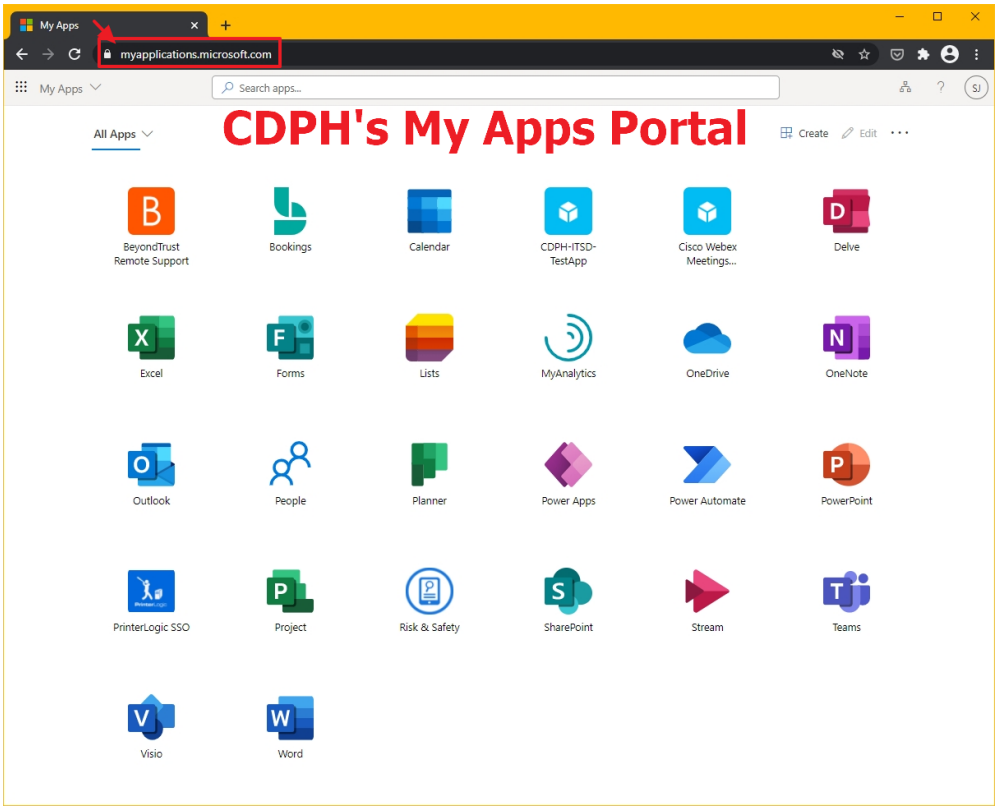
The workflow process below illustrates how a user can send a request and a business unit manager can approve the request through My Apps. The end result of this workflow approval / denial process that the user has either has access to the requested resource or denied access to the resource.

Proposed CDPH Group Membership Request and Approval Process

Note that everything that happens with Azure AD is logged, and that includes changes to groups and group membership. Auditing can be performed in real time, along with monitoring and alerting on sensitive activities originating from a specific group.

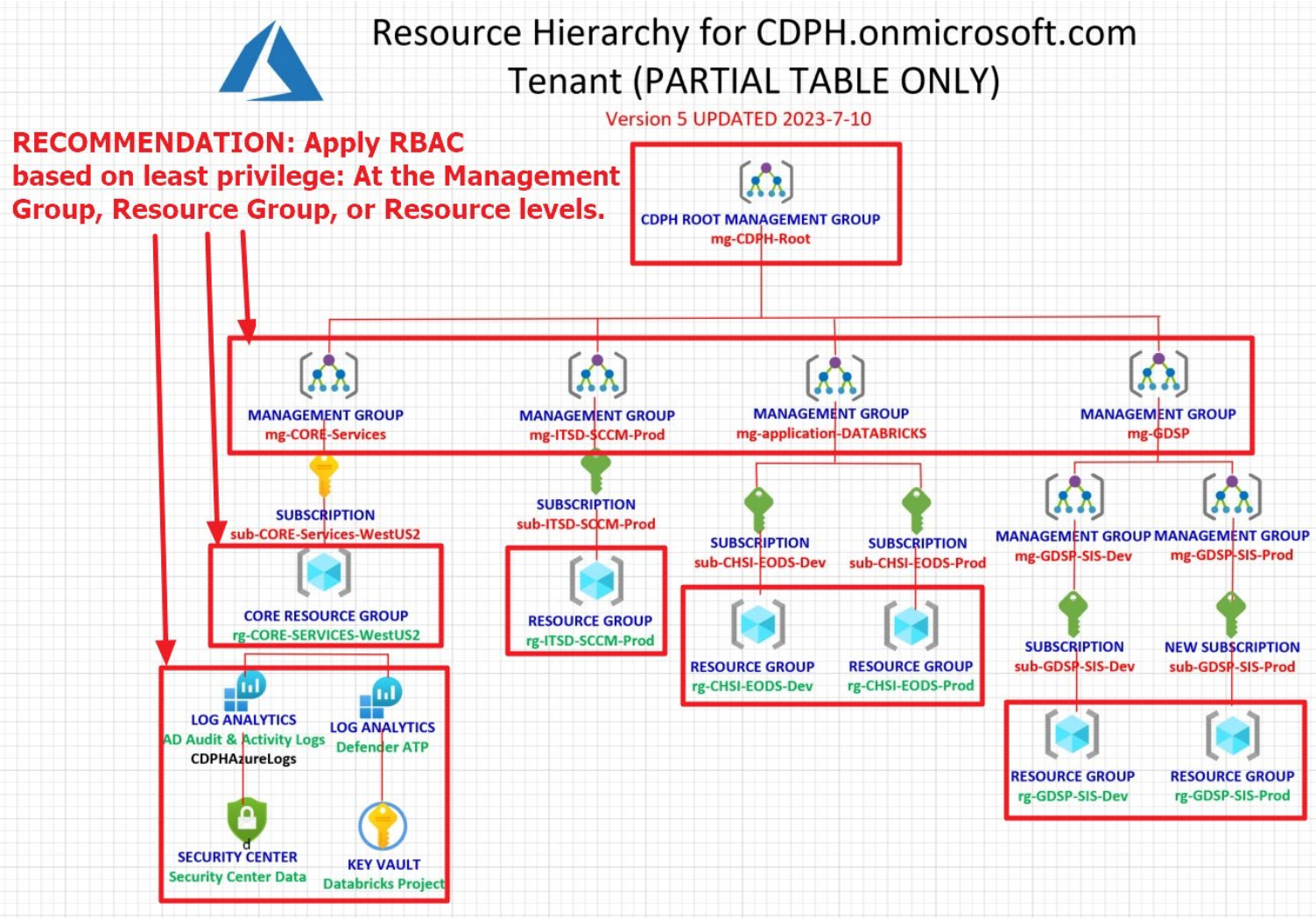
FOR DISCUSSION: On-prem AD groups cannot be used for self-service group membership; however, this is on the roadmap and will be supported in the future (timeline uncertain). Will CDPH use cloud AD groups in the interim?

The screen shot below shows what CDPH's My Apps portal looks like to a non-administrative user. Note that the "groups" option is not shown as CDPH currently has self-service group membership disabled.



(UPDATED 2023-7-10 by Shayaan Motamedi): The Key to Successful and Efficient RBAC: Scoping at the Appropriate Level Following Principle of Least Privilege

As a best practice, CDPH will assign RBAC scoped at the appropriate level following the principle of least privileged access. It is important to note that RBAC permissions are inherited from higher levels; permissions that are applied at the management group level are inherited by the subscriptions, resource groups, and resources that are below it. RBAC should be scoped at the management group level if it is appropriate for that access to be inherited by the scopes below it. If RBAC needs to be more granular and only give access to specific subscriptions, resource groups, or resources, then apply the RBAC at the appropriate level following the principle of least privileged access while noting the inheritance structure.

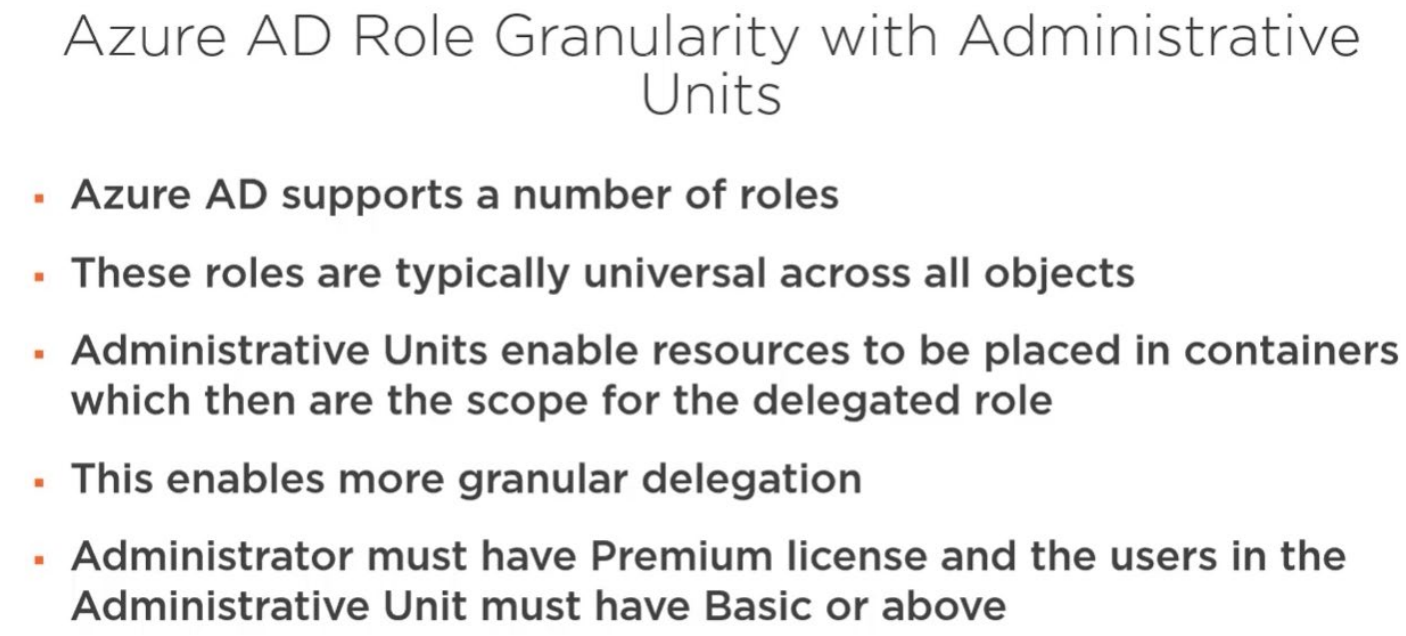


Administrative Units: For situations that require more granular delegation

For the past 22 years, Active Directory has used Organizational Units (OUs) to logically partition the directory. This partitioning capability has not been available to Azure until the launch of Administrative Units (AU) for public preview in April 2020 and now, this feature is generally available.

An Administrative Unit is an Azure AD resource that can be a container for other Azure AD resources. Unlike Management Groups, an Administrative Unit can contain users and groups for now but may extend to other resources in the future (timeline undetermined).

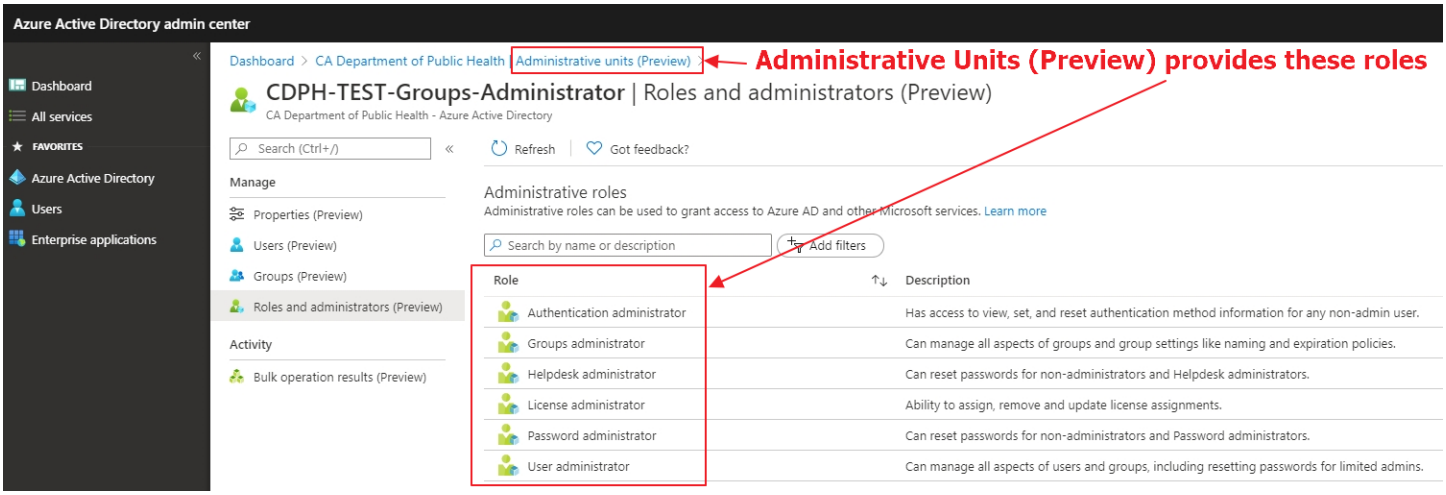
Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the Helpdesk Administrator role to regional support specialists, so they can manage users only in the region that they support.



Considerations to using Administrative Units (AUs):

- Only users who are Global Admins or Privileged Role Admins can create AUs.
- Group Assignment to AUs is not straightforward as you cannot assign them in bulk. If you need to add or remove three groups, for example, you need to add or remove each one individually.
- **LIMITED ROLES**: Only the following roles are available for AUs:
    - **Authentication Administrator**
      Has access to view, set, and reset authentication method information for any non-admin user in the assigned Administrative Unit only.
    - **Groups Administrator**
      Can manage all aspects of groups and groups settings like naming and expiration policies in the assigned Administrative Unit only.
    - **Helpdesk Administrator**
      Can reset passwords for non-administrators and Helpdesk administrators in the assigned Administrative Unit only.
    - **License Administrator**
      Can assign, remove, and update license assignments within the Administrative Unit only.
    - **Password Administrator**
      Can reset passwords for non-administrators and Password Administrators within the assigned Administrative Unit only.
- **User Administrator**
  Can manage all aspects of users and groups, including resetting passwords for limited admins within the assigned Administrative Unit only.

The screen shot below illustrates the limited roles available:

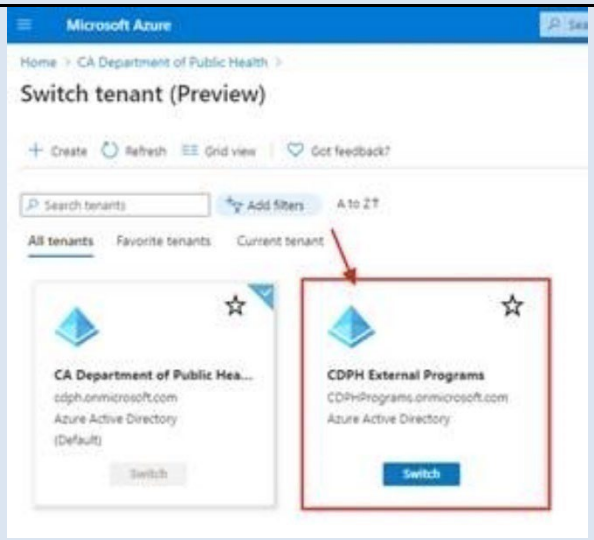


6. A use-case scenario for Administrative Units is to limit administrative privileges. This documentation illustrates the steps necessary to accomplish the goal:

MANAGING AZURE GROUPS USING ADMINISTRATIVE UNITS TO LIMIT ADMINISRATIVE PRIVILEGES

OBJECTIVE: The group "SIS Prod MFA Enabled" is currently managed by users with excessive privileg including the delete privilege. This document will leverage the use of Administrative Units to more granularly assign privileges. This will limit the scope of administrative permissions.

PREREQUISITE:

Appropriate minimum permission CDPHPrograms.onmicrosoft.com tenant that will allow for creation of Administrative Units: Privileged Role Administrator	

STEP 1:

Access the portal for the CDPHPrograms.onmicrosoft.com B2B tenant.

Note the owners of SIS Prod MFA Enable group.

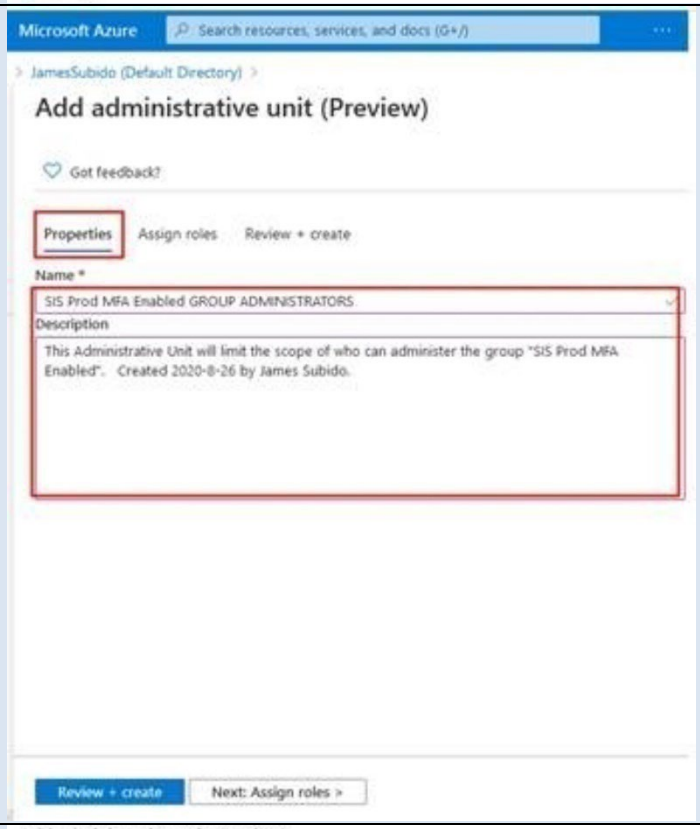
STEP 2:

Add an Administrative Unit and use a descriptive name.

Examples:
SIS Prod MFA Enabled GROUP ADMINISTRATORS

Or

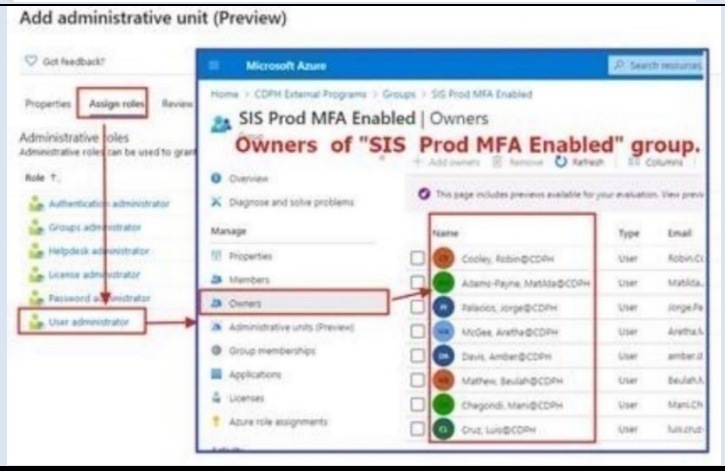
ADMINISTRATORS for the SIS Prod MFA Enabled GROUP

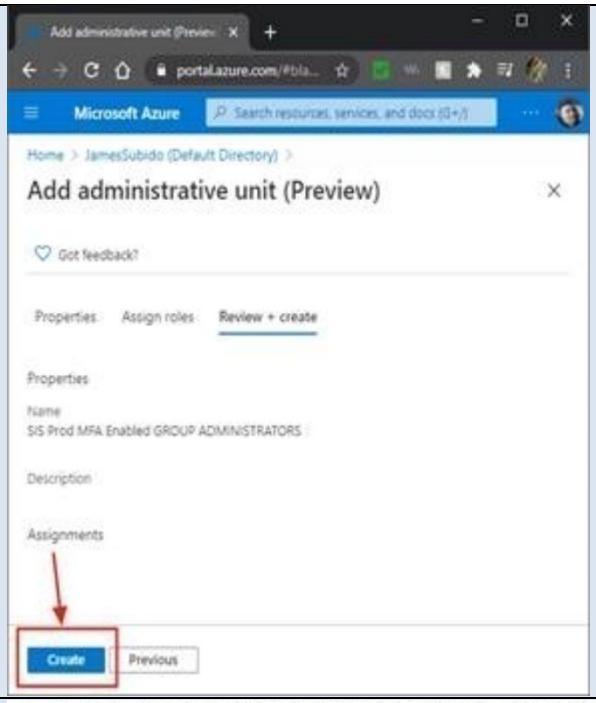


STEP 3:

KEY STEP: Assign all the owners of the Prod MFA Enabled Group with "User Administrator" role.

This role and the privileges it delegates w limited in scope to the SIS Prod MFA Enab group only.

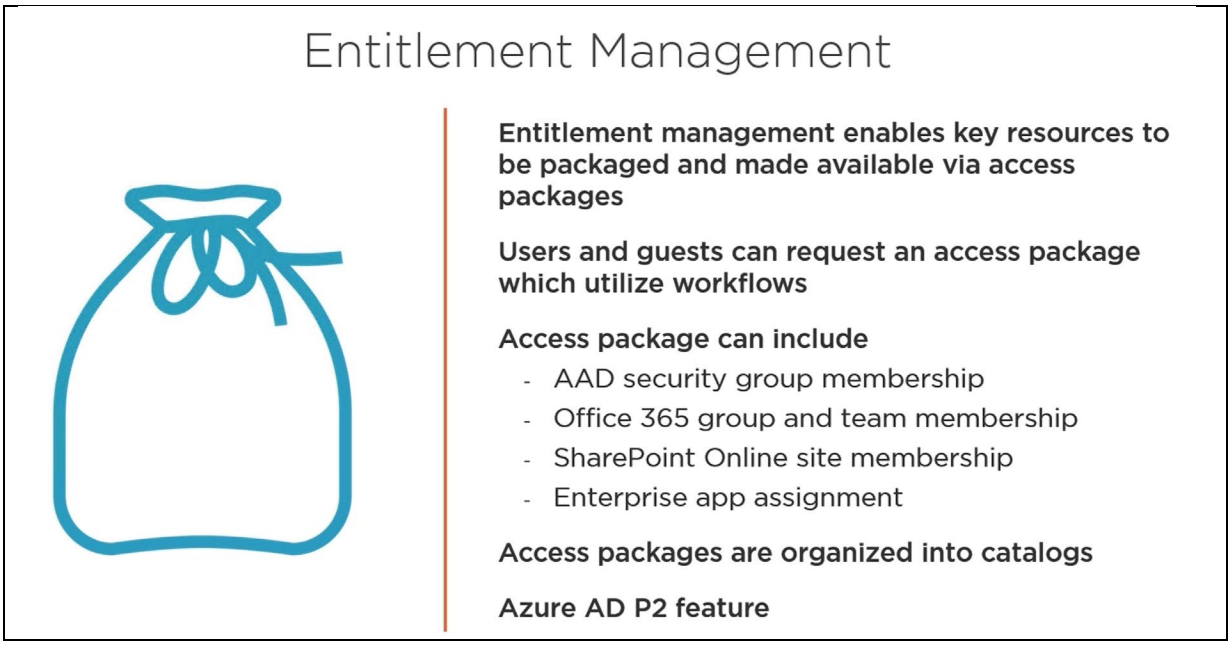


STEP 4: Click **"Create"** to crate the new Administr Unit.	
STEP 5: Edit the properties of the new Administrat unit by **adding the group SIS Prod MFA Enabled**. Note that Users remain empty.	
STEP 6: **CLEAN-UP STEP:** Remove these users fr ownership of SIS Prod MFA Enabled grou	

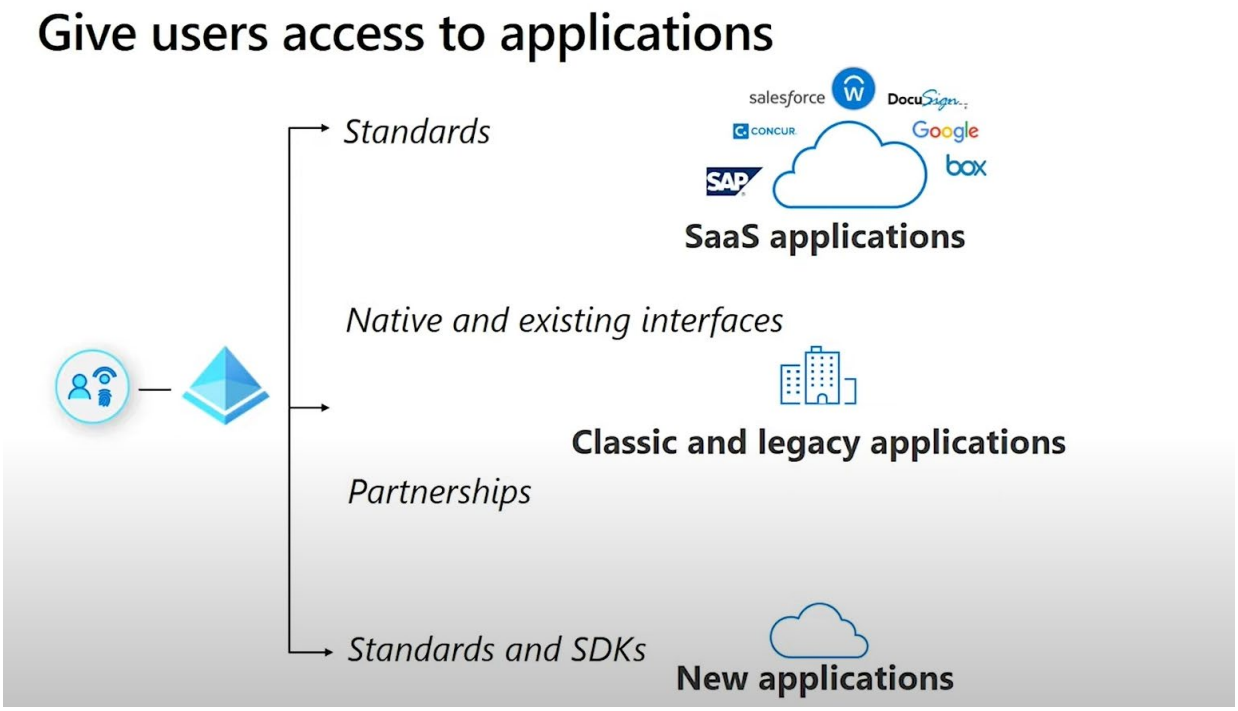
7. Identity Governance: Entitlement Management

An Azure AD Identity Governance feature, Entitlement Management removes barriers to internal and external collaboration by automating employee and partner access requests, approvals, auditing, and

review. Entitlement Management provides administrators the ability to create, automate, and categorically group together necessary resources into what is called an access package.



An Access Package can provide access to Azure AD security group memberships, Office 365 group and team membership, SharePoint Online site membership, and applications such as SaaS applications, classic and legacy applications, and new applications as shown in the screen shot below:



KEY TAKE-AWAY: Note that Access Packages can also provide the requestor with memberships to CDPH's AD groups, which in turn gives them access to Azure RBAC privileges. Access Packages do not always need to provide access just to applications.

Entitlement Management provides delegation capabilities and offloads access requests to CDPH business unit managers without burdening the IT staff with every access request. It empowers users to request access to resources they need. Just like the discussion on self-service group management from the precious section on RBAC, CDPH business unit managers can review and approve access requests.

Security comes in the form of policies -- user scoping, required approval, and expiration lifecycle ensure that only the right people have the right access for the right amount of time, limiting access risk.

When removing access, guest account clean-up is automatic -- users are removed from the directory when they no longer have access to the package. Removing access can be a manual or automatic (based on lifecycle expiration date).

CDPH Workflow

The workflow below leverages Microsoft's design principle that delegates business unit managers the ability to define the Access Package resources and policies in collaboration with CDPH Azure IT Admins. The workflow begins with CDPH Azure IT Admins' creation of an AD security group that provides CDPH business unit managers (who are non-administrators) the ability to create a catalogue in which the Access Package will reside.

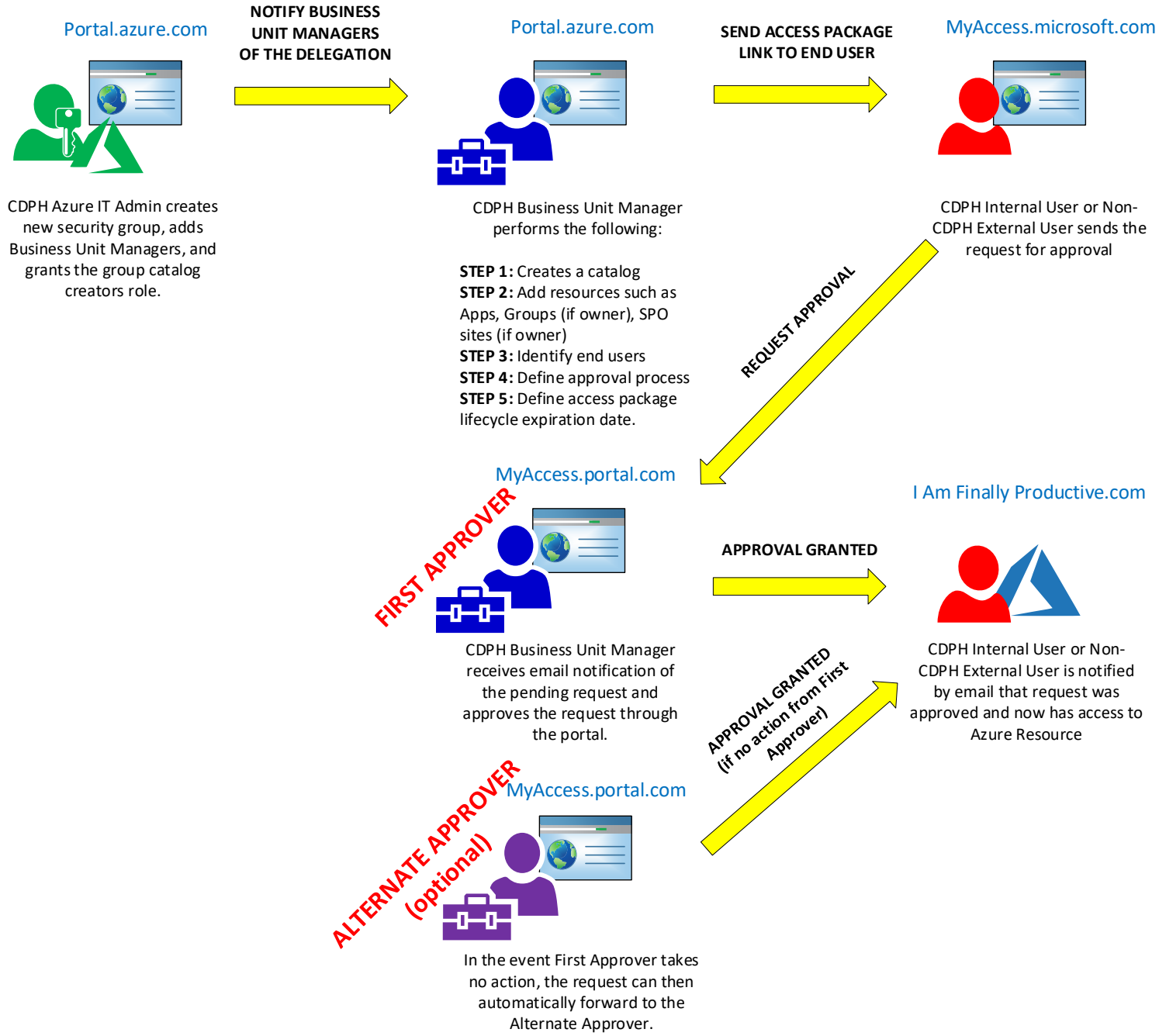
Next, the IT Admin notifies the business unit manager of the delegation and delegates the tasks of creating the Access Package with the business unit manager. Note that this process may be completely offloaded to the manager or may be performed as a collaborative effort between the two.

Steps 3-5 constitute the Access Package policy, which allows the manager to define a) who can request access; b) the approval process; c) and the expiration lifecycle.

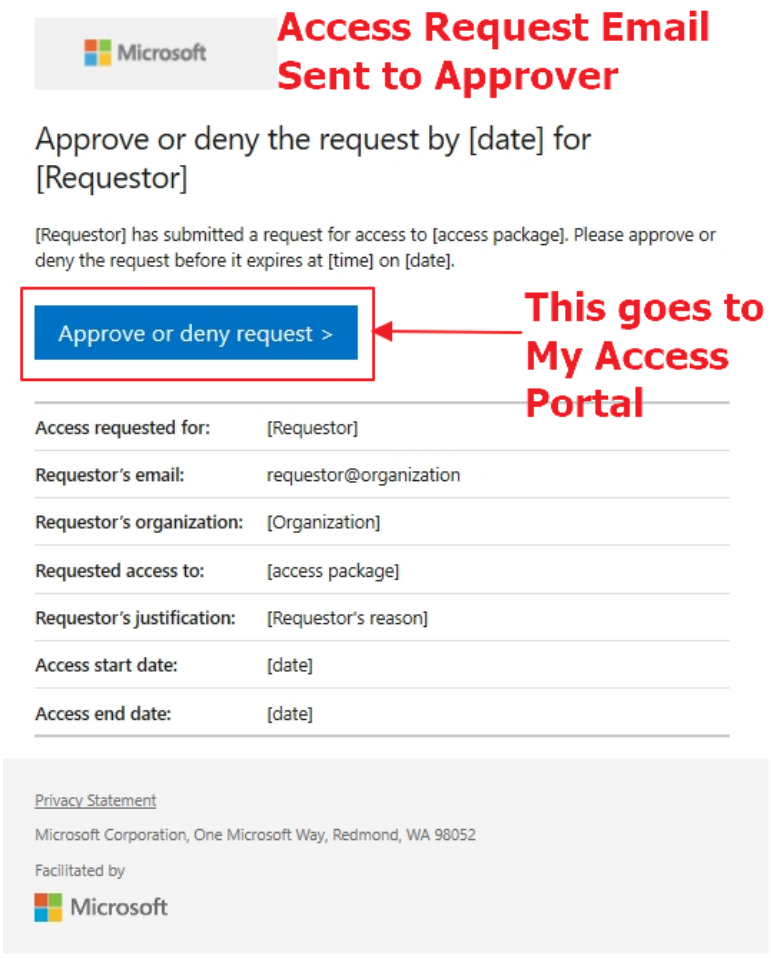
The requestor (internal or external user) receives an email which includes a link to the My Access Portal (https://myaccess.microsoft.com). A request for approval to a business unit manager (first approver) with an optional backup manager in the event the first approver is unable to act. Once approval is granted, the user has access to the resource.

The Visio provisioning workflow below illustrates the process:

Proposed CDPH Entitlement Management Process



The screen shot below shows the email triggered by the end user which is sent to the business unit manager to approve or deny the request.



UPDATE: December 15, 2021: Access Package Creation Procedure

HOW TO CREATE AN ACCESS PACKAGE

An Access Package is a bundle of resources that a project needs and is governed with policies. Access Packages are defied in containers called Catalogs. When we add a Business Unit Manager as a member of the Catalog Owner RBAC Group, that manager has the ability:

- To add and remove users associated with the RBAC group associated with each Access Package.
- Perform periodic Access Reviews for each Access Package.

PREREQUISITES:

1) Make sure you have a Catalog Owner RBAC group created and populated appropriately.

GROUP	WHAT IS THE GROUP FOR?	
rbac-ITSD-ESS-Snowflake-CalConnect-cat-CatalogOwner	This group will be used for Catalog ownership, RBAC Group management (add/remove users), and Access Reviews. It is named after the catalog for which it is the designated owner. This group will contain: 1) Business owner 2) Business owner's assistant 3) ESS staff (at least two) We will call this "**The Catalog Owner RBAC Group**"	

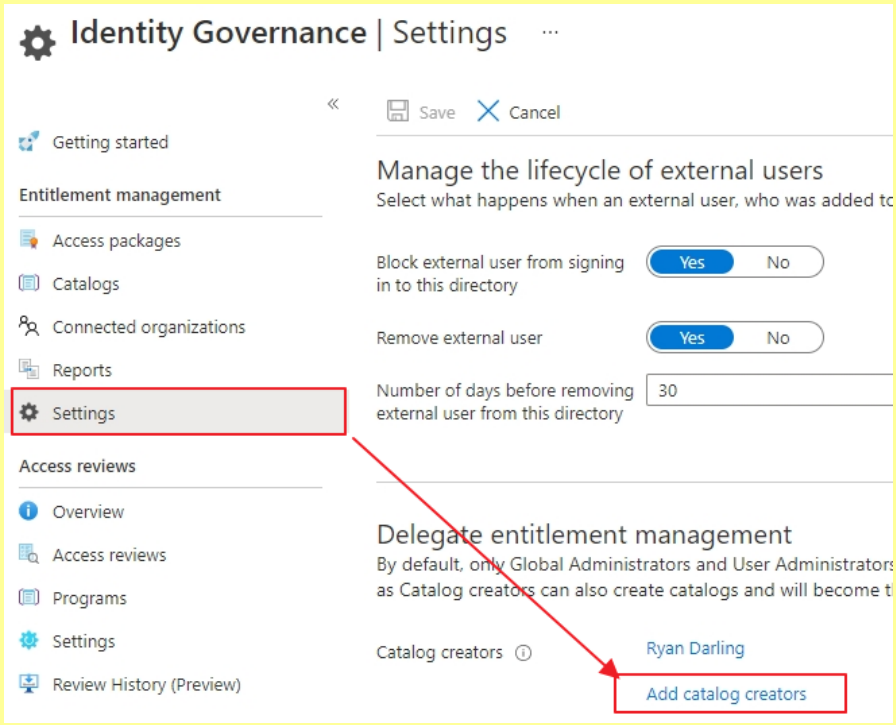
2) Make sure you have an RBAC Group created and populated appropriately.

The whole point of an Access Package is to allow the Business Manager to add or remove users from the RBAC group. The remainder of this document will use the San Joaquin Prod Read RBAC group as an example.

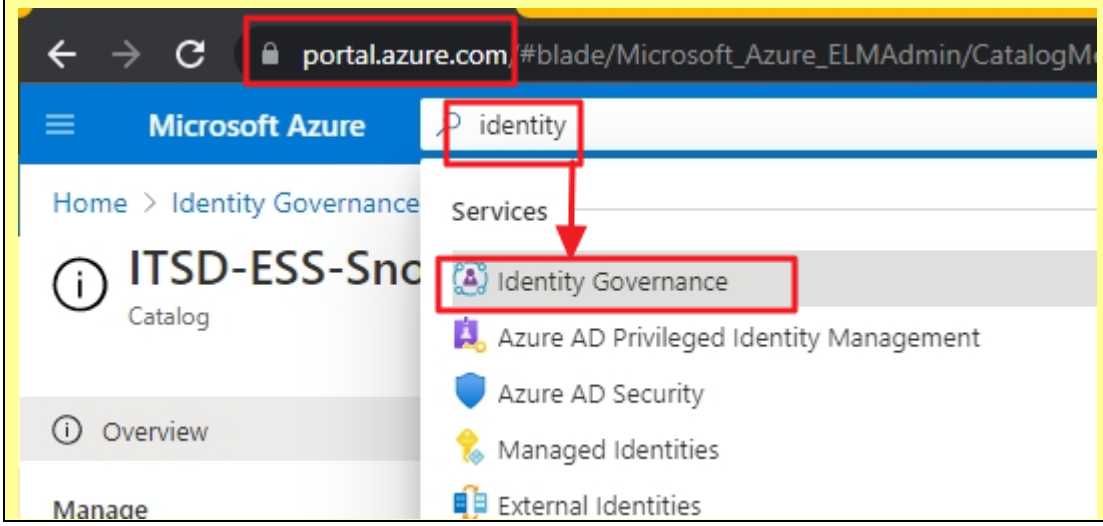
GROUP	WHAT IS THE GROUP FOR?
RBAC_CID_DCDC_CALCONNECT_EA_SNOWFLAKE_CDPH_SANJOAQUIN_PROD_READ	This group will contain t end-users that will be assigned roles within Snowflake. We will call this "**The RBAC Group**"

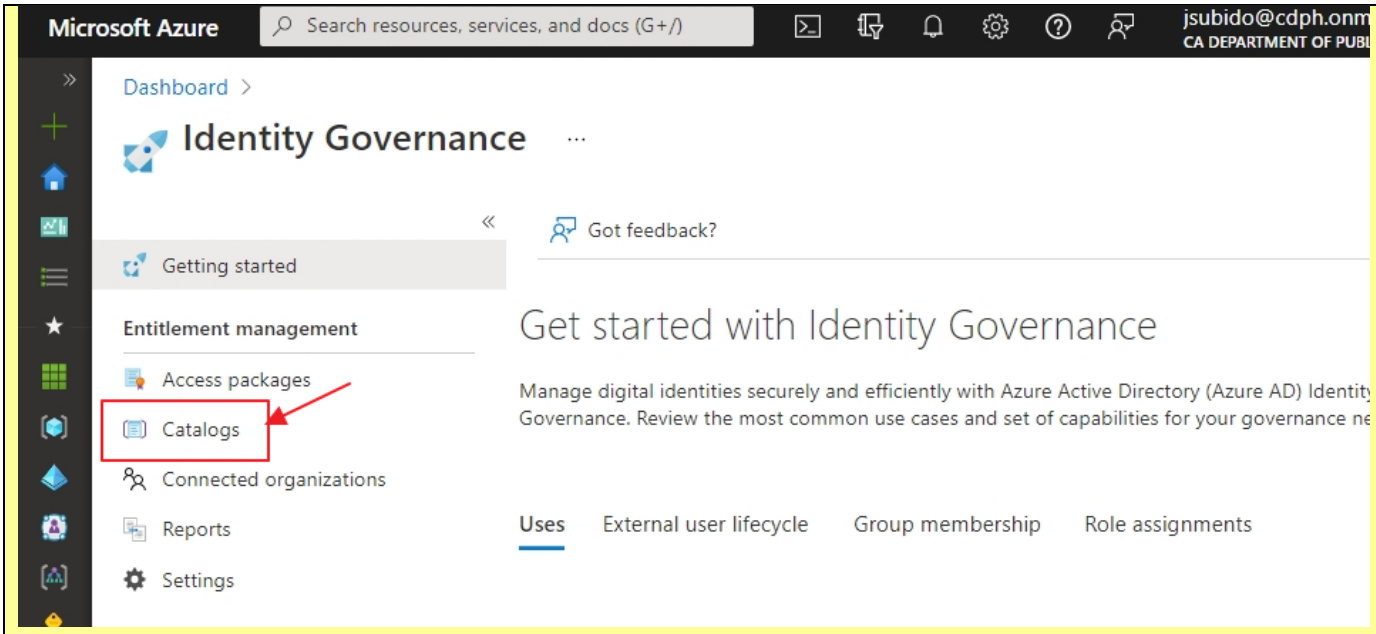
3) Catalog Creator Privilege Required

The ESS staff who will be creating the Catalog will be required to have the "Catalog Creators" entitlement. Any Azure Administrator with Global Administrator privilege can delegate this entitlement to ESS staff.

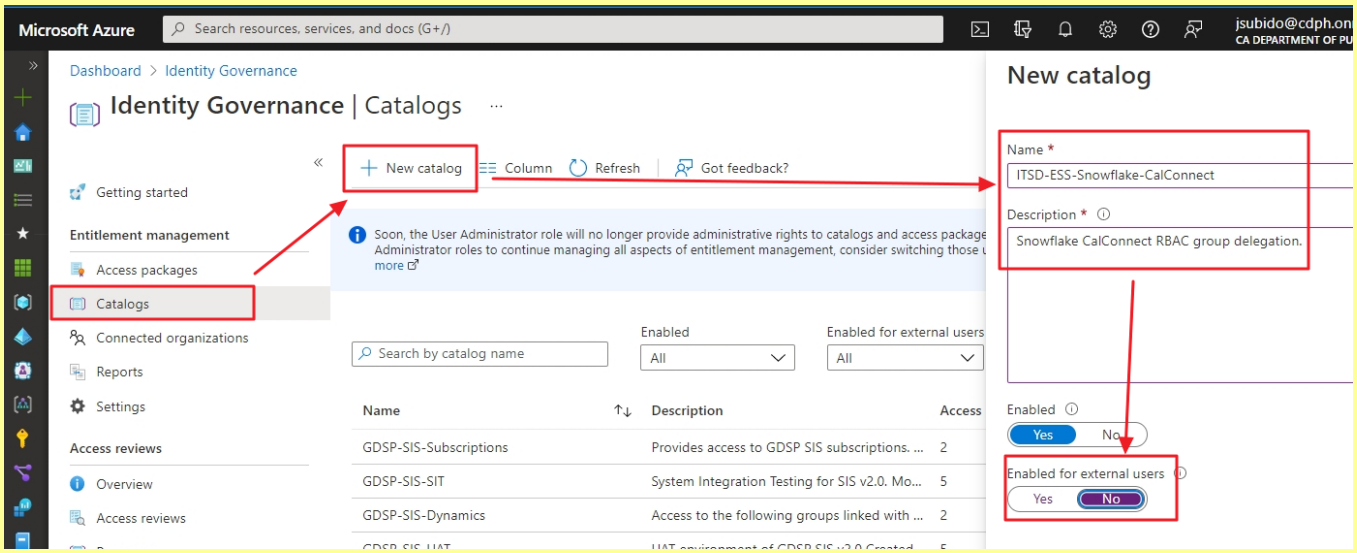


STEP 1: ESS STAFF Create a Catalog



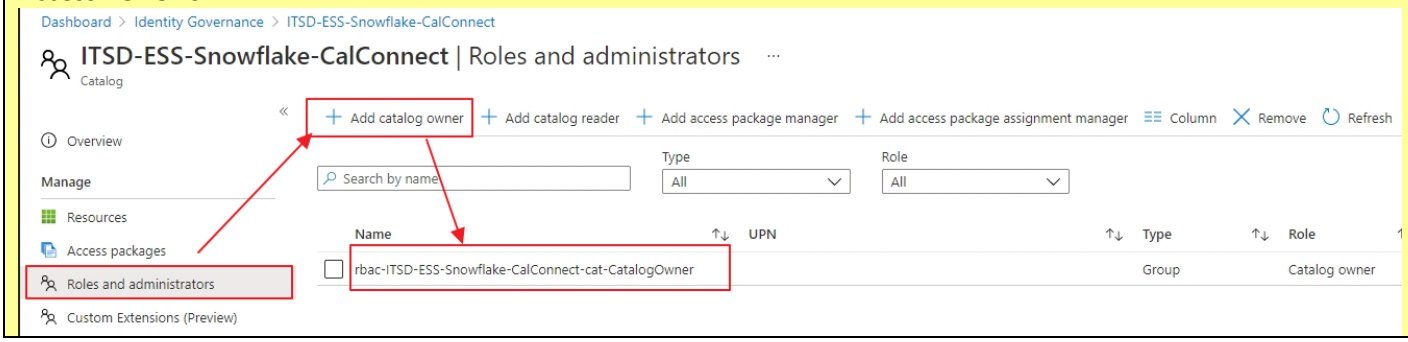


Create the new catalog.

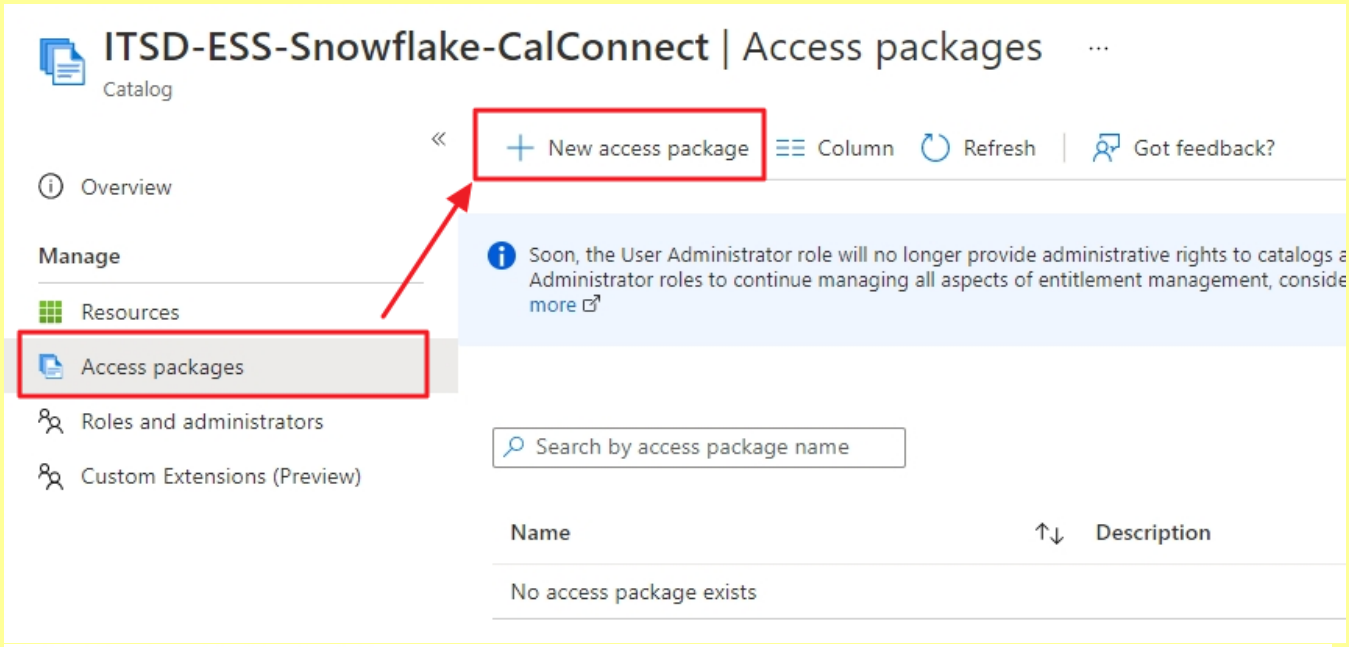


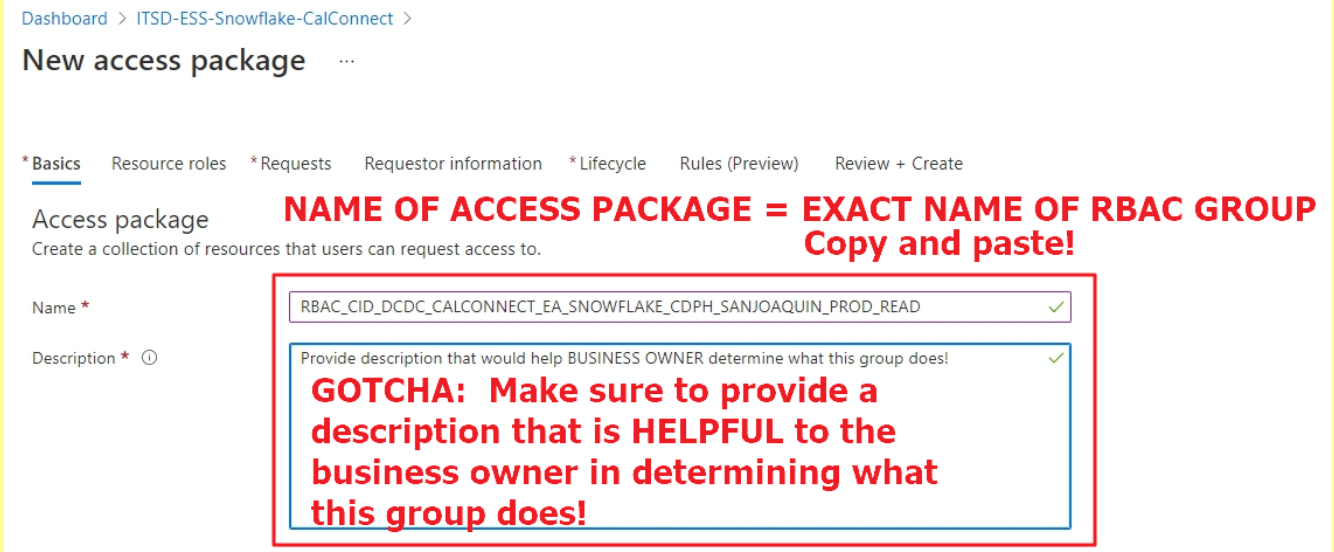
Add the catalog owner

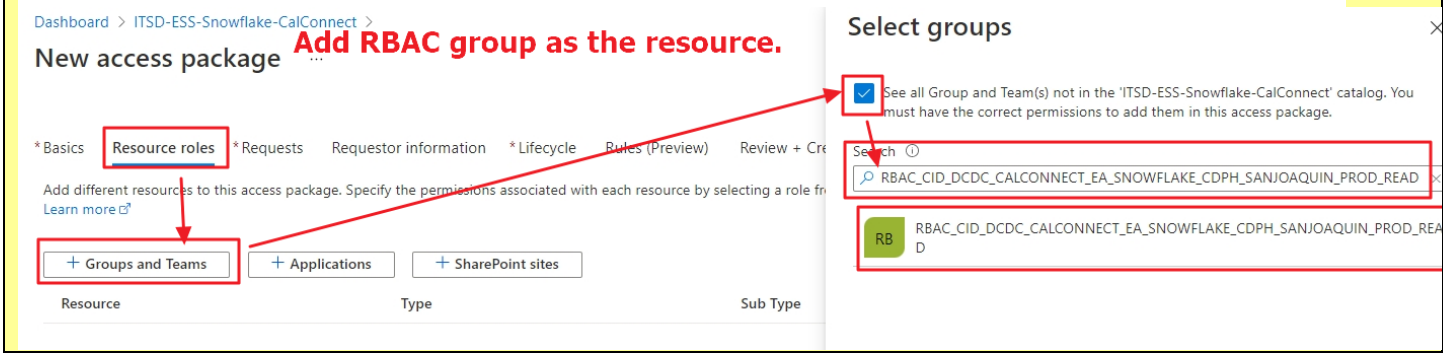
The prerequisite requires the creation of the group rbac-ITSD-ESS-Snowflake-CalConnect-cat-CatalogOwner
so that we can identify members of this group as the owner of the catalog and will be responsible for performing Access Reviews.

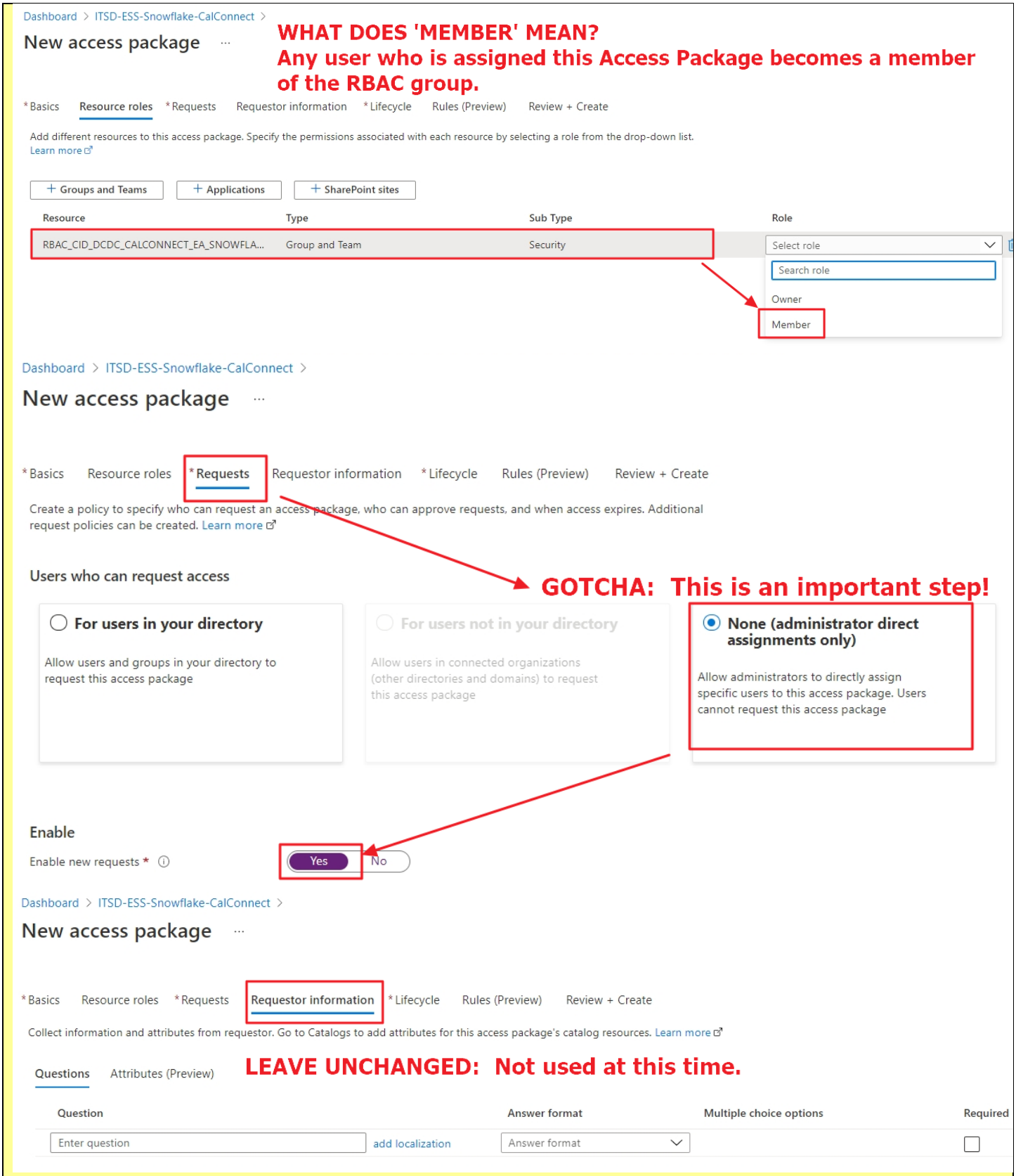


STEP 2: ESS STAFF Create an Access Package

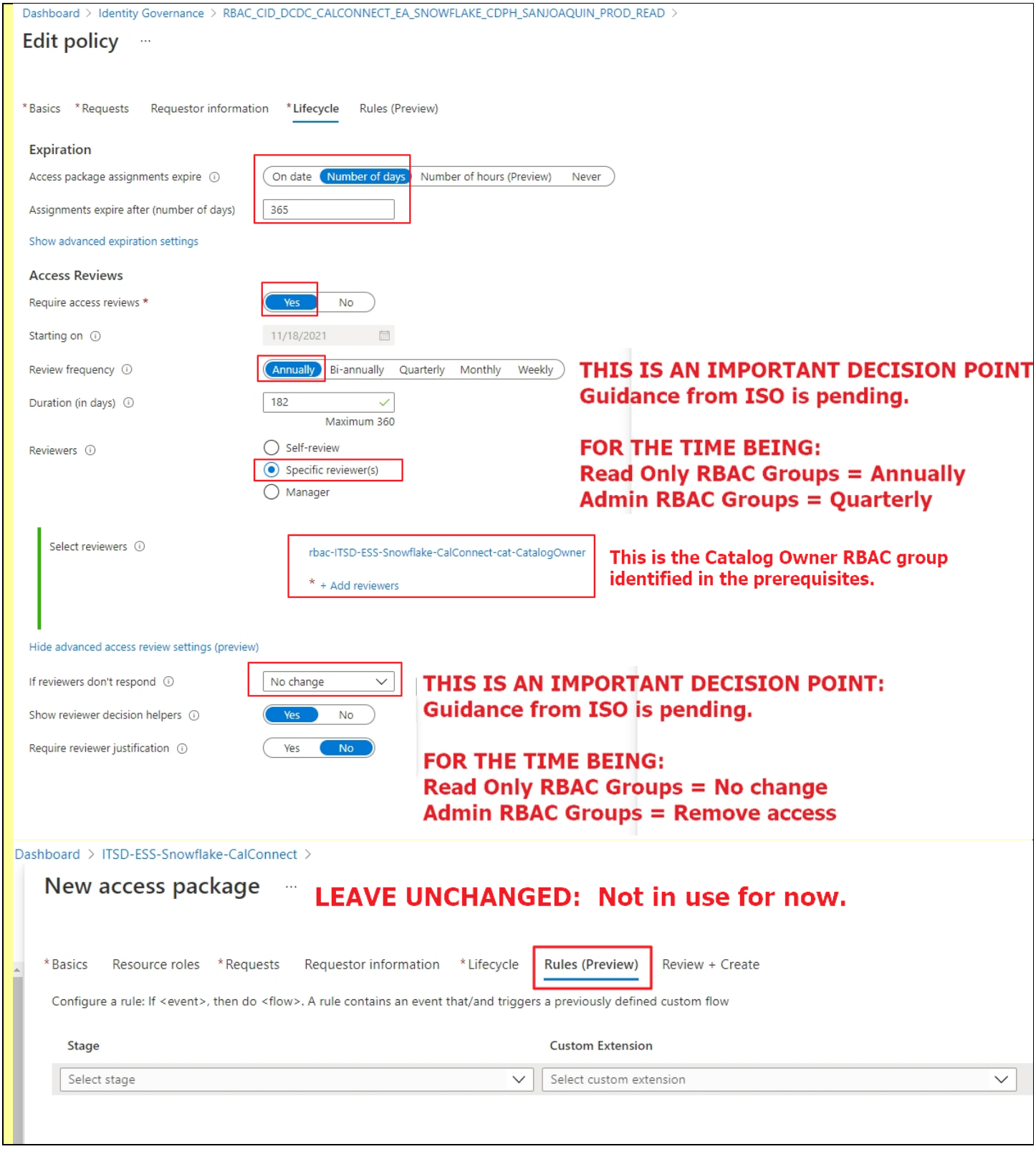


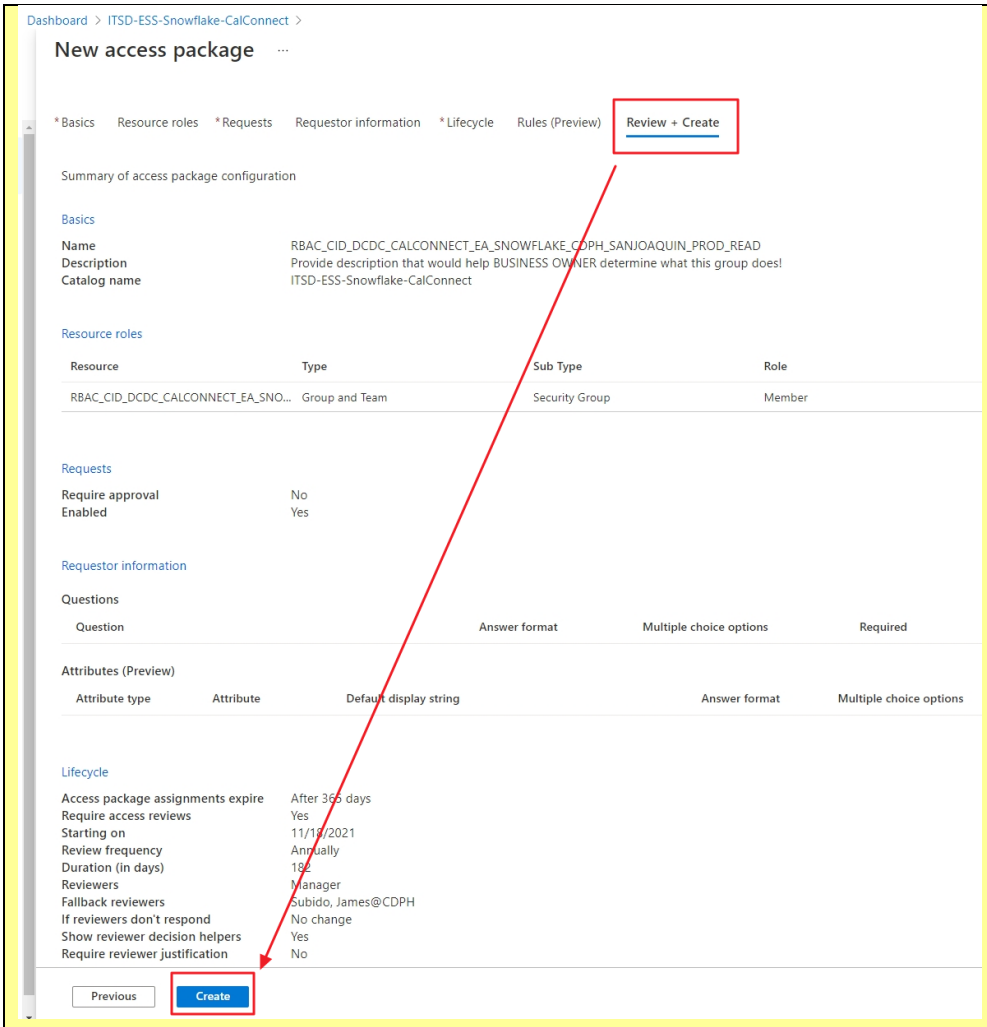






ACCESS REVIEW: Requires ISO Guidance

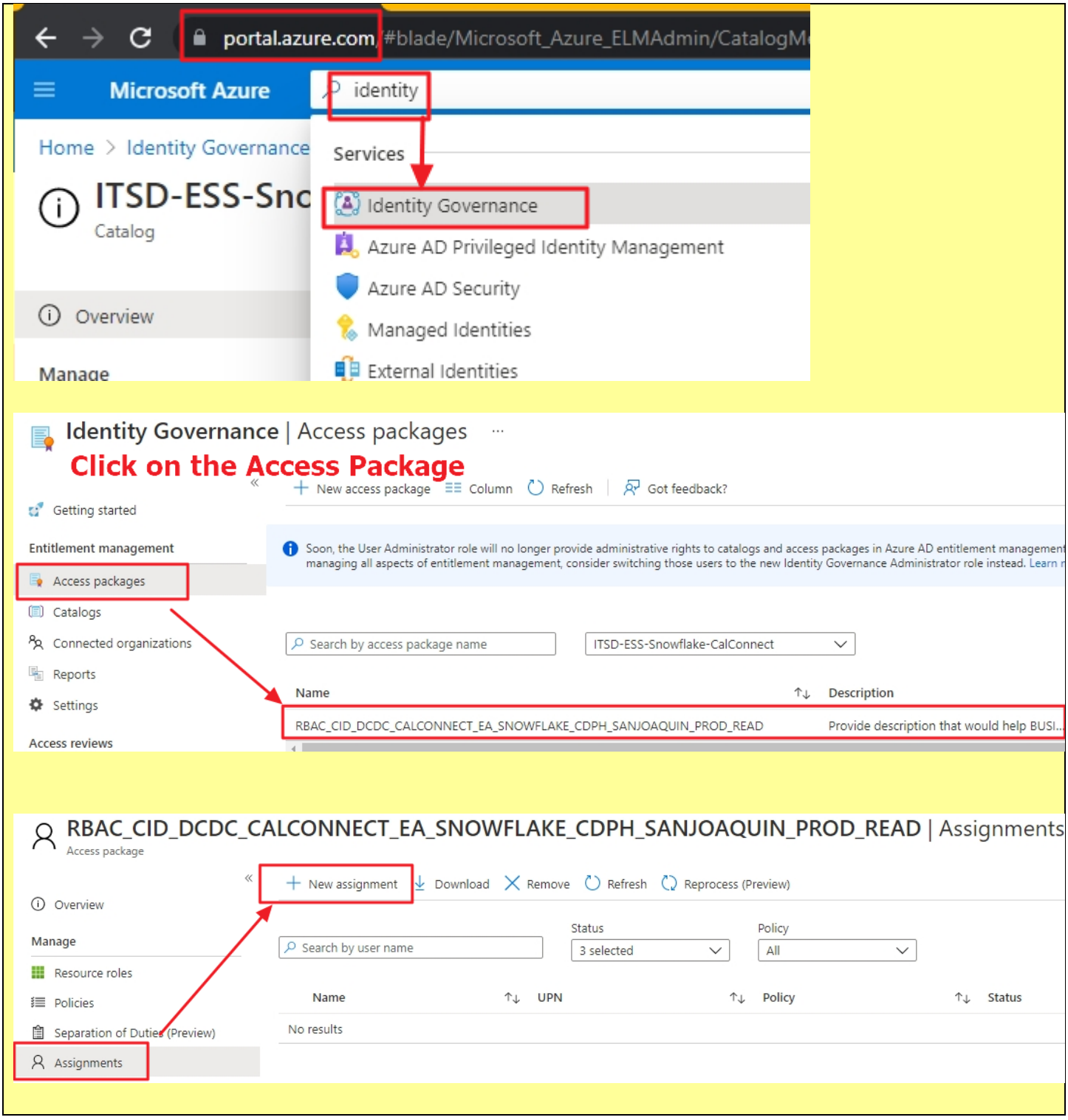

Dashboard > Identity Governance > RBAC_CID_DCDC_CALCONNECT_EA_SNOWFLAKE_CDPH_SANJOAQUIN_PROD_READ >
Edit policy
*Basics *Requests Requestor information *Lifecycle Rules (Preview)
Expiration
Access package assignments expire
On date Number of days Number of hours (Preview) Never
Assignments expire after (number of days)
365
Show advanced expiration settings
Access Reviews
Require access reviews *
Yes No
Starting on
11/18/2021
Review frequency
Annually Bi-annually Quarterly Monthly Weekly
Duration (in days)
182
Maximum 360
Reviewers
Self-review
Specific reviewer(s)
Manager
THIS IS AN IMPORTANT DECISION POINT
Guidance from ISO is pending.
FOR THE TIME BEING:
Read Only RBAC Groups = Annually
Admin RBAC Groups = Quarterly
Select reviewers
rbac-ITSD-ESS-Snowflake-CalConnect-cat-CatalogOwner
* + Add reviewers
This is the Catalog Owner RBAC group identified in the prerequisites.
Hide advanced access review settings (preview)
If reviewers don't respond
No change
Show reviewer decision helpers
Yes No
Require reviewer justification
Yes No
THIS IS AN IMPORTANT DECISION POINT:
Guidance from ISO is pending.
FOR THE TIME BEING:
Read Only RBAC Groups = No change
Admin RBAC Groups = Remove access
Dashboard > ITSD-ESS-Snowflake-CalConnect >
New access package
LEAVE UNCHANGED: Not in use for now.
*Basics Resource roles *Requests Requestor information *Lifecycle Rules (Preview) Review + Create
Configure a rule: If <event>, then do <flow>. A rule contains an event that/and triggers a previously defined custom flow
Stage
Custom Extension
Select stage
Select custom extension

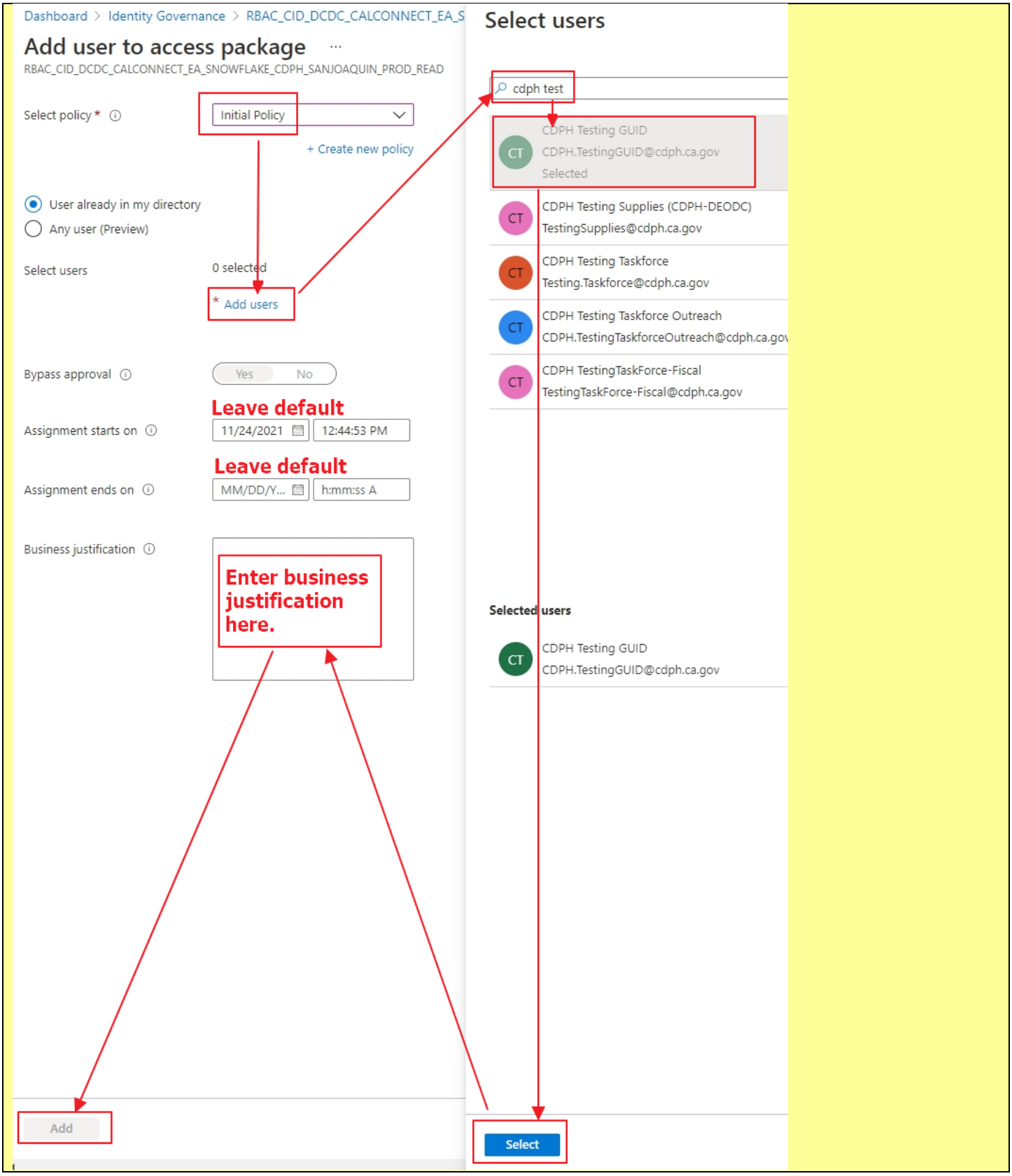


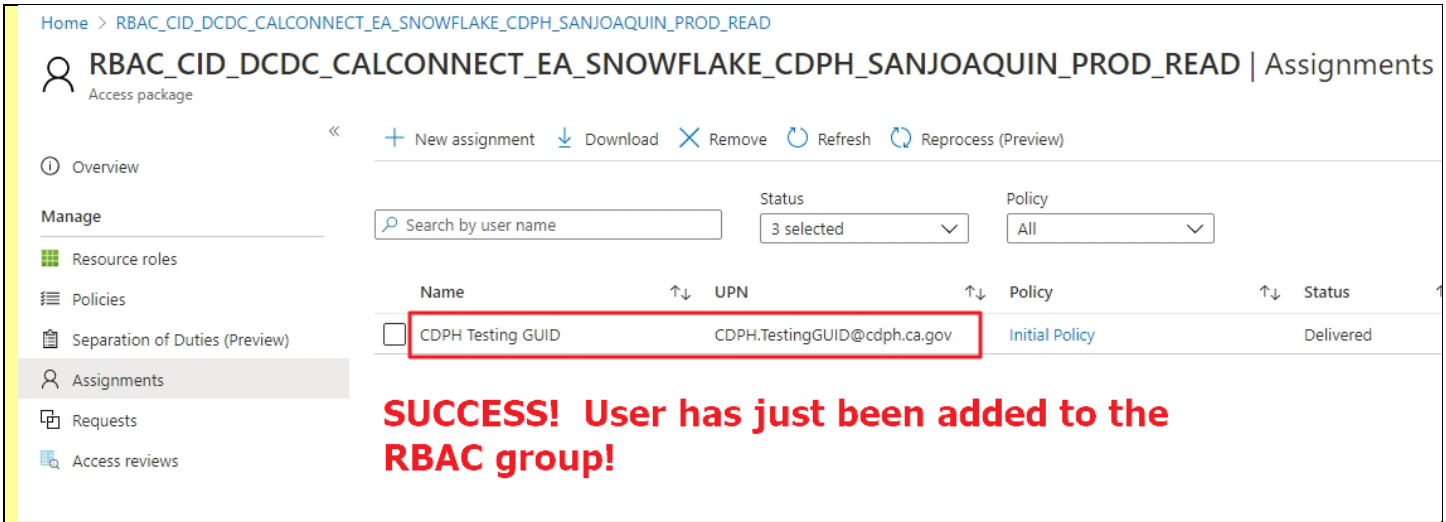
1. BUSINESS UNIT MANAGER: ASSIGNING ACCESS PACKAGES

PREREQUISITE:

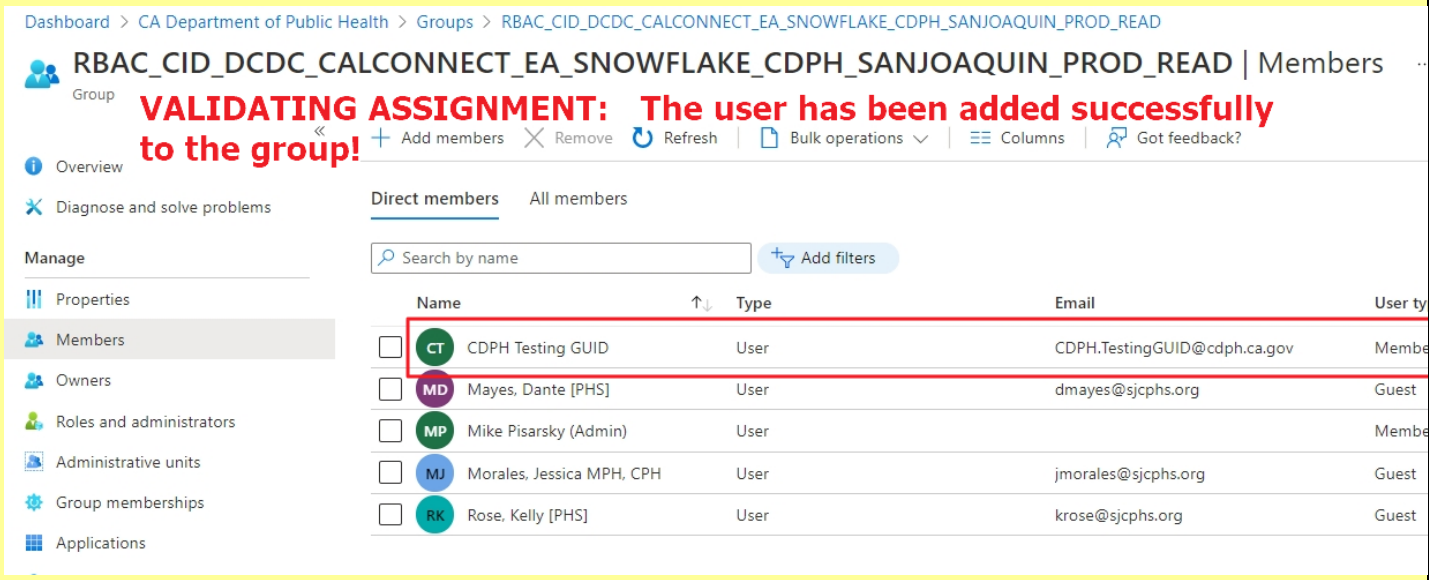
ESS Staff creates a catalog that contains at least one Access Package. The Business Unit Manager is a member of the Catalog RBAC group **rbac-ITSD-ESS-Snowflake-CalConnect-cat-CatalogOwner**


portal.azure.com/#blade/Microsoft_Azure_ELMAdmin/CatalogM
Microsoft Azure
identity
Home > Identity Governance
Services
ITSD-ESS-Snc
Catalog
Identity Governance
Azure AD Privileged Identity Management
Azure AD Security
Managed Identities
External Identities
Overview
Manage
Identity Governance | Access packages
Click on the Access Package
New access package
Column
Refresh
Got feedback?
Getting started
Entitlement management
Access packages
Catalogs
Connected organizations
Reports
Settings
Access reviews
Soon, the User Administrator role will no longer provide administrative rights to catalogs and access packages in Azure AD entitlement management
managing all aspects of entitlement management, consider switching those users to the new Identity Governance Administrator role instead.
Search by access package name
ITSD-ESS-Snowflake-CalConnect
Name
Description
RBAC_CID_DCDC_CALCONNECT_EA_SNOWFLAKE_CDPH_SANJOAQUIN_PROD_READ
Provide description that would help BUSI...
RBAC_CID_DCDC_CALCONNECT_EA_SNOWFLAKE_CDPH_SANJOAQUIN_PROD_READ | Assignments
Access package
New assignment
Download
Remove
Refresh
Reprocess (Preview)
Overview
Manage
Resource roles
Policies
Separation of Duties (Preview)
Assignments
Search by user name
Status
3 selected
Policy
All
Name
UPN
Policy
Status
No results

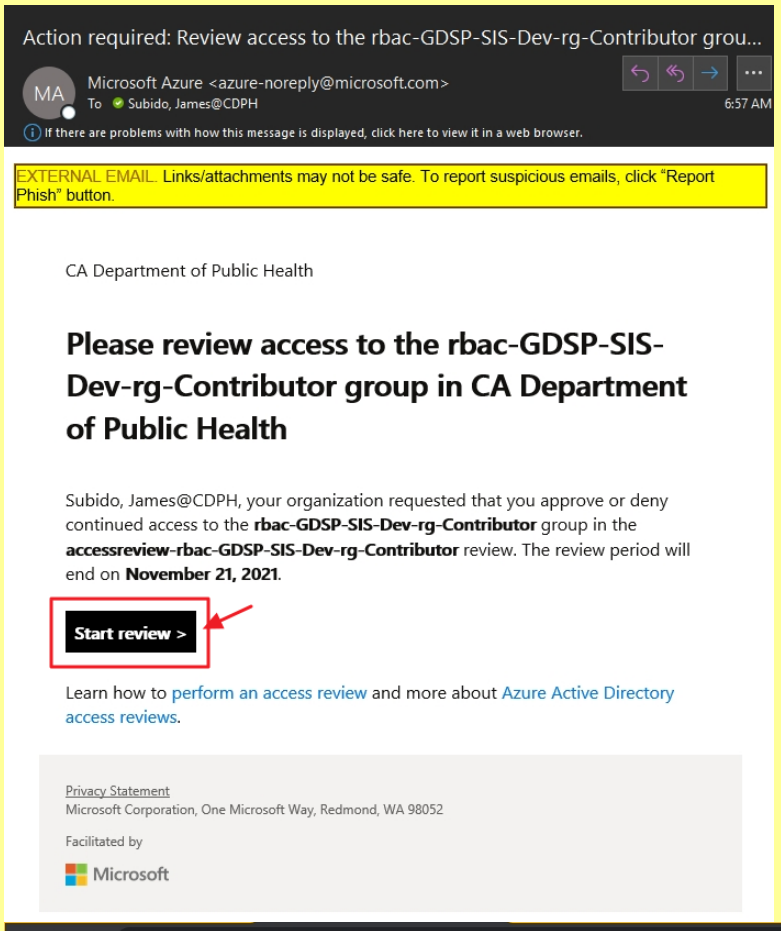

Dashboard > Identity Governance > RBAC_CID_DCDC_CALCONNECT_EA_S
Add user to access package
RBAC_CID_DCDC_CALCONNECT_EA_SNOWFLAKE_CDPH_SANJOAQUIN_PROD_READ
Select policy *
Initial Policy
+ Create new policy
User already in my directory
Any user (Preview)
Select users
0 selected
* Add users
Bypass approval
Yes
No
Leave default
Assignment starts on
11/24/2021
12:44:53 PM
Leave default
Assignment ends on
MM/DD/Y...
h:mm:ss A
Business justification
Enter business justification here.
Add
Select users
cdph test
CDPH Testing GUID
CDPH.TestingGUID@cdph.ca.gov
Selected
CDPH Testing Supplies (CDPH-DEODC)
TestingSupplies@cdph.ca.gov
CDPH Testing Taskforce
Testing.Taskforce@cdph.ca.gov
CDPH Testing Taskforce Outreach
CDPH.TestingTaskforceOutreach@cdph.ca.gov
CDPH TestingTaskForce-Fiscal
TestingTaskForce-Fiscal@cdph.ca.gov
Selected users
CDPH Testing GUID
CDPH.TestingGUID@cdph.ca.gov
Select

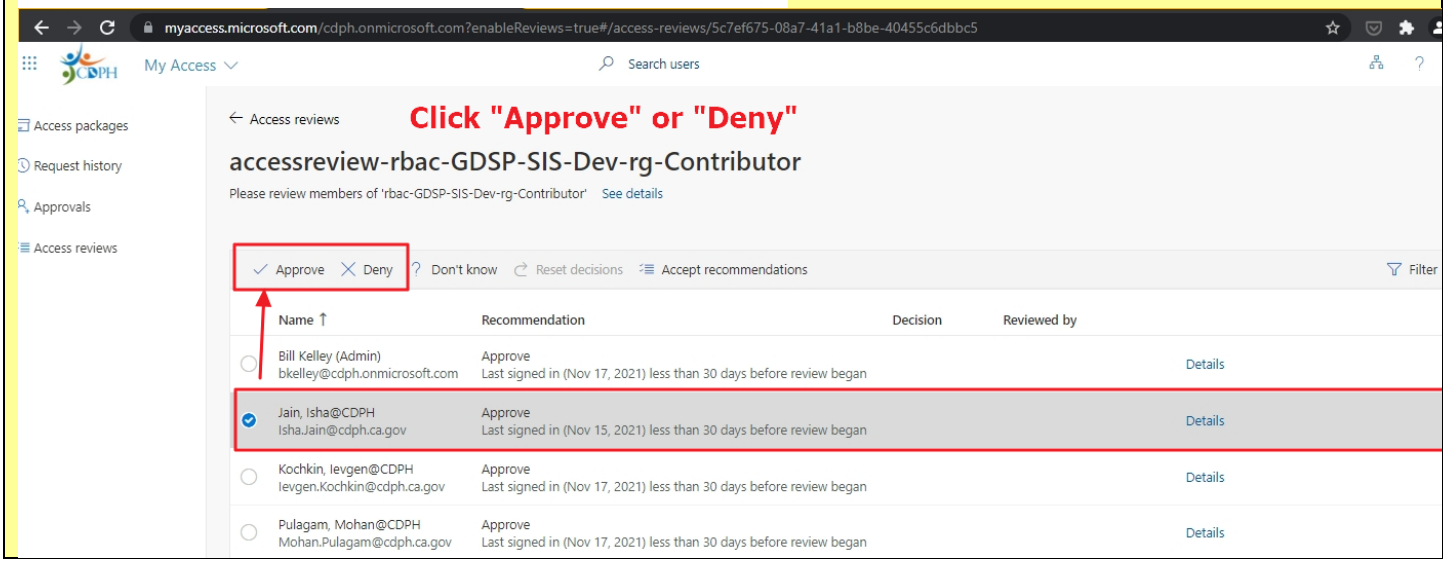


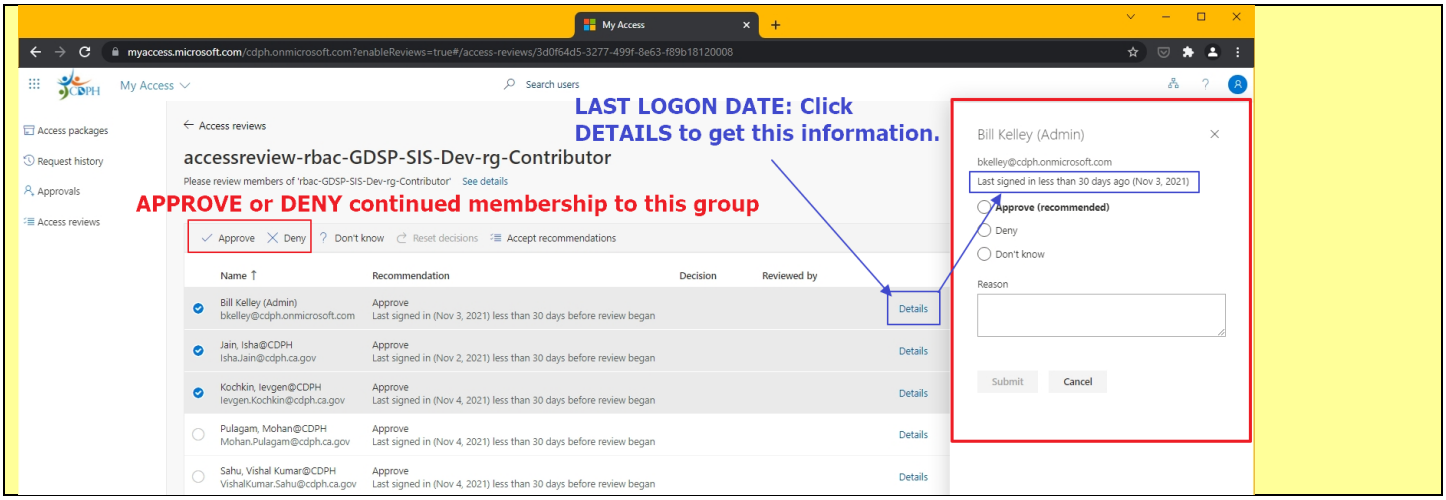
HOW DO WE VALIDATE? To verify the assignment, ESS can bring up the members of the RBAC group in Azure AD.



2. BUSINESS UNIT MANAGER: ACCESS REVIEW PROCESS







Use Case Scenario

Here is another possible use case for Entitlement Management: providing access to Power BI reports for external CDT users.

POSSIBLE USE CASE FOR ENTITLEMENT MANAGEMENT

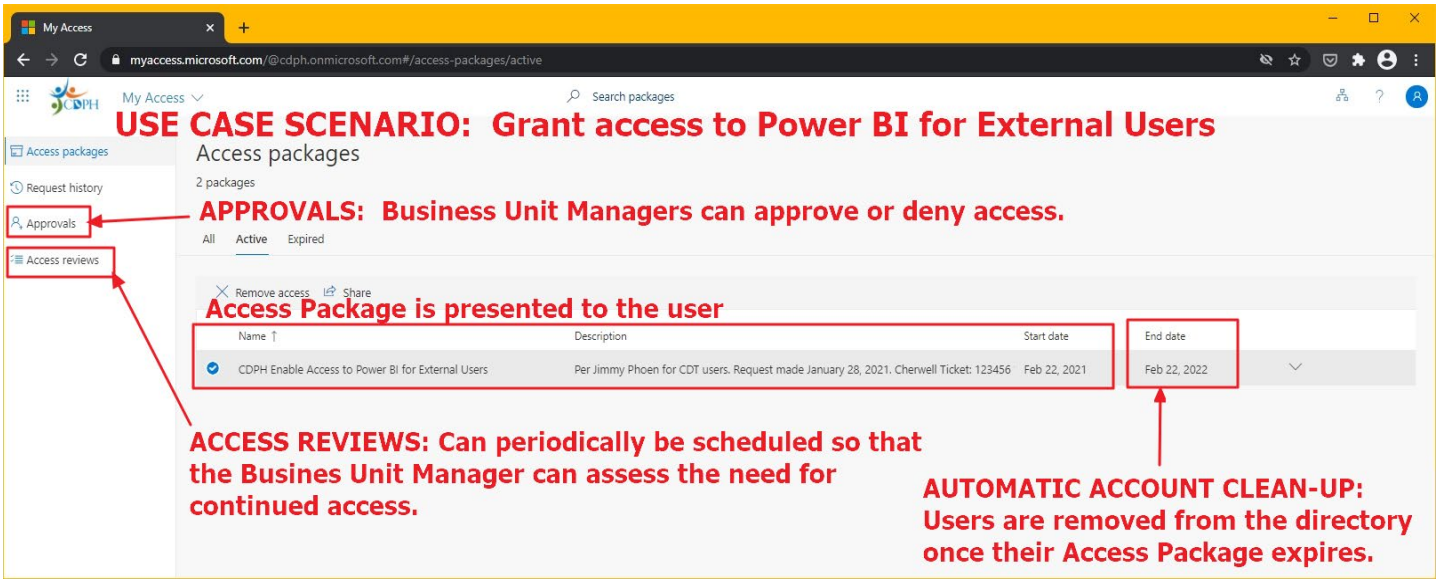
From: Phoen, Jimmy@CDPH <Jimmy.Phoen@cdph.ca.gov>
Sent: Thursday, January 28, 2021 10:25 AM
To: Benson, Tyrone@CDPH <Tyrone.Benson@cdph.ca.gov>
Cc: Stewart, Ryan@CDPH <Ryan.Stewart@cdph.ca.gov>; Banister, Richard@CDPH <Richard.Banister@cdph.ca.gov>; Giles, Theresa@CDPH <Theresa.Giles@cdph.ca.gov>
Subject: PowerBI report access from external users

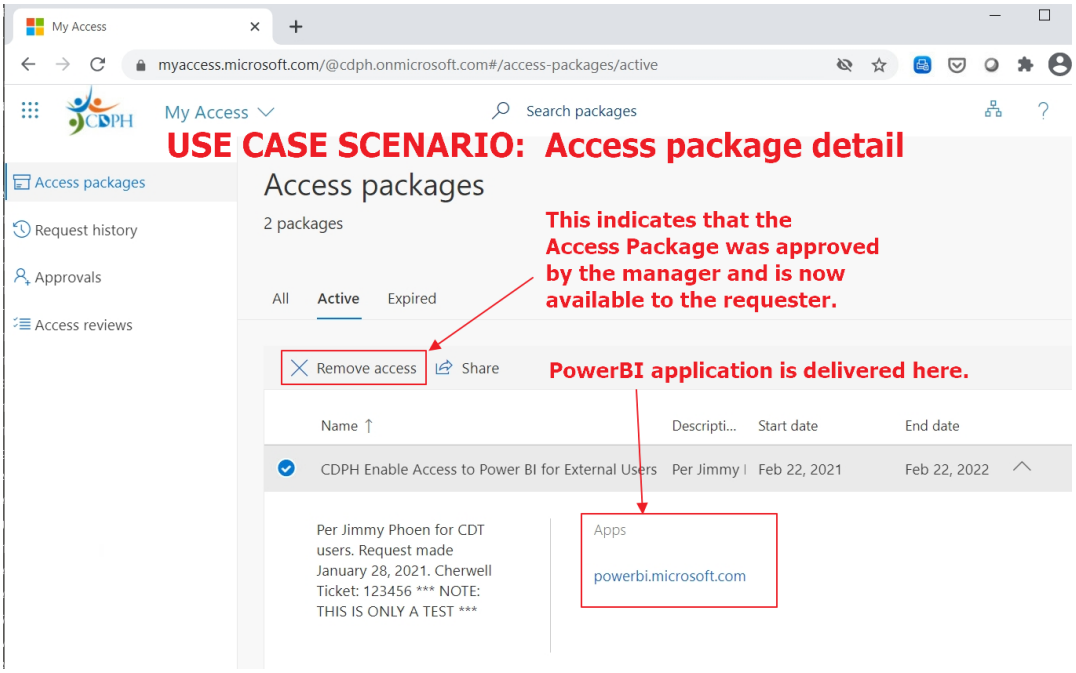
Hi Tyrone,

We have a use case where we need to allow users from external users to view powerBI reports (specifically CDT users). From what I read, we need to be "Invite external users to your organization" on the powerBI tenant settings. And then restrictions to only allow CDT domain on Azure Active Directory for PowerBI application.

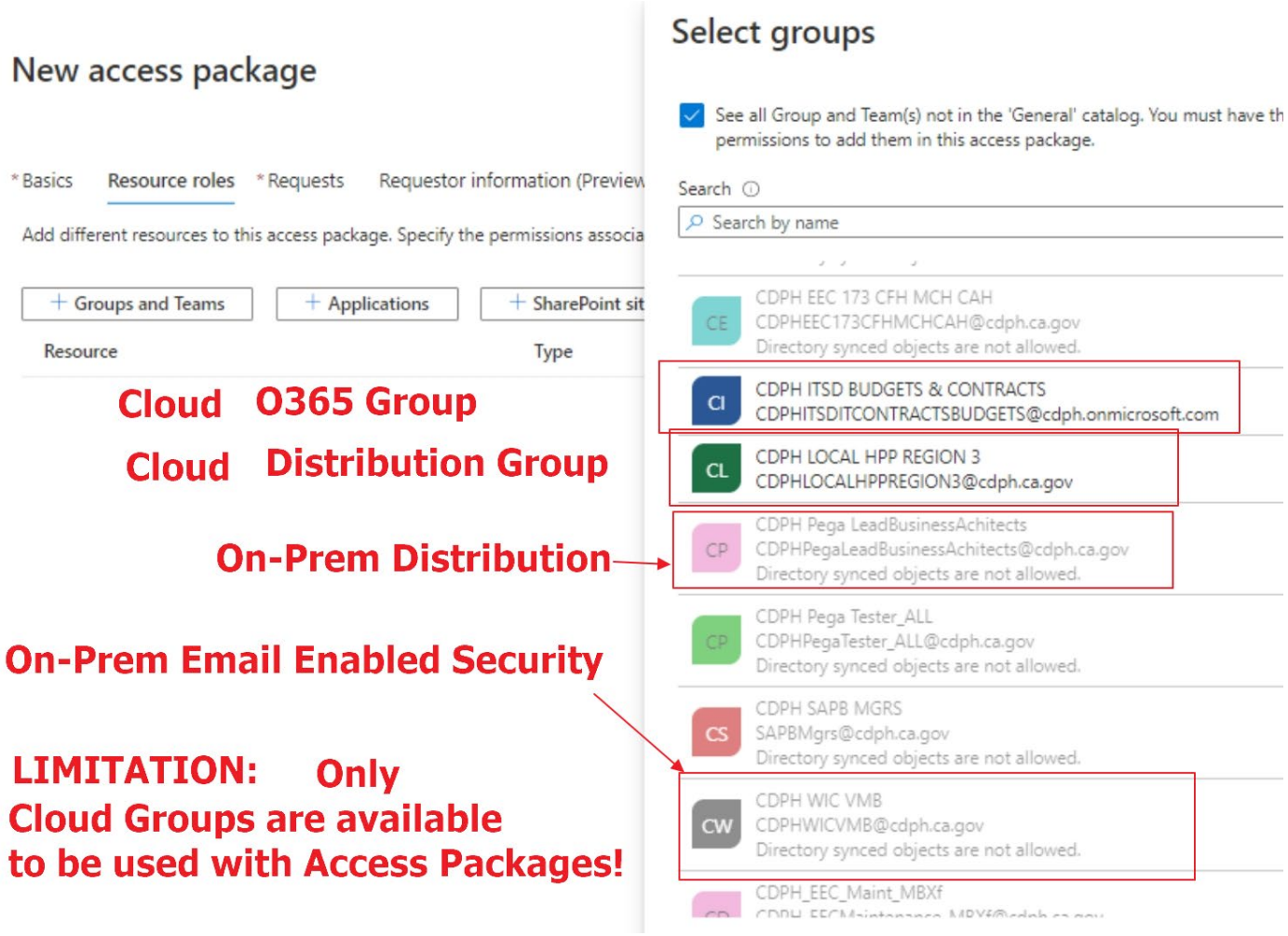
Is this something you can help us with?

Here is a sample Access Package for the above-mentioned use case. Note the various elements associated with the Access Package such as approvals, Access Reviews (discussed in a later section), and expiration date. The user clicks on the Access Package and initiates the request process which the business unit manager will have to approve.





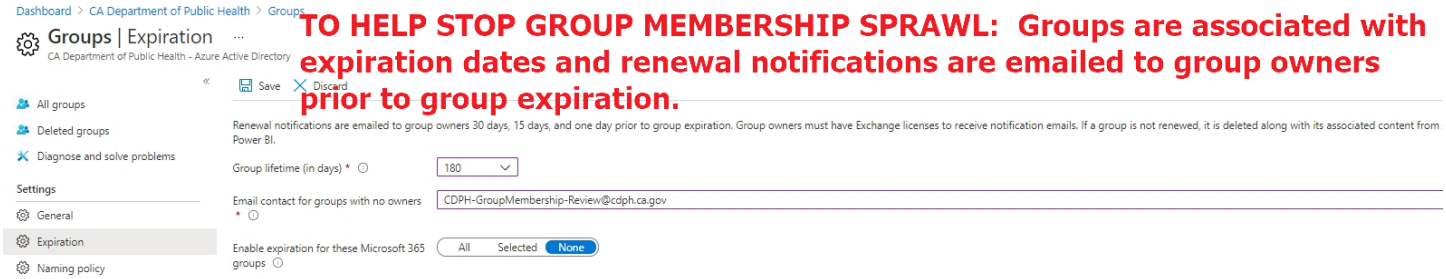
The screen shot below notes the current limitation on the use of groups with Access Packages: only AD groups created and maintained in the cloud are supported.



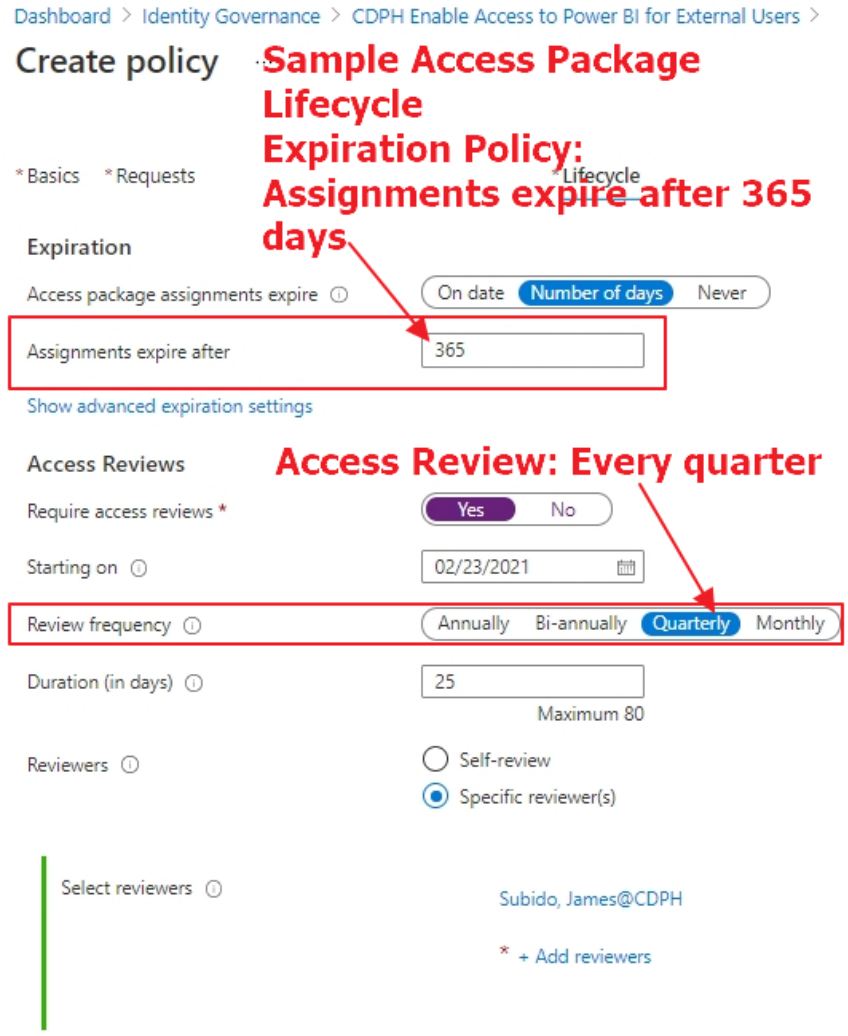
FOR DISCUSSION: CDPH will need to create new Azure AD groups in order to use Entitlement Management. What will be the naming convention for these new groups? Perhaps we need to consider that groups containing external guest users need to be reflected in the naming convention.

Automatic Expiration of Access

Since CDPH's on-prem AD groups are not set to expire, a policy for setting AD groups created on Azure AD to set to expire may be worth considering. With the idea that every Azure AD group has an owner, establishing an expiration date for AD groups may help to control membership sprawl.



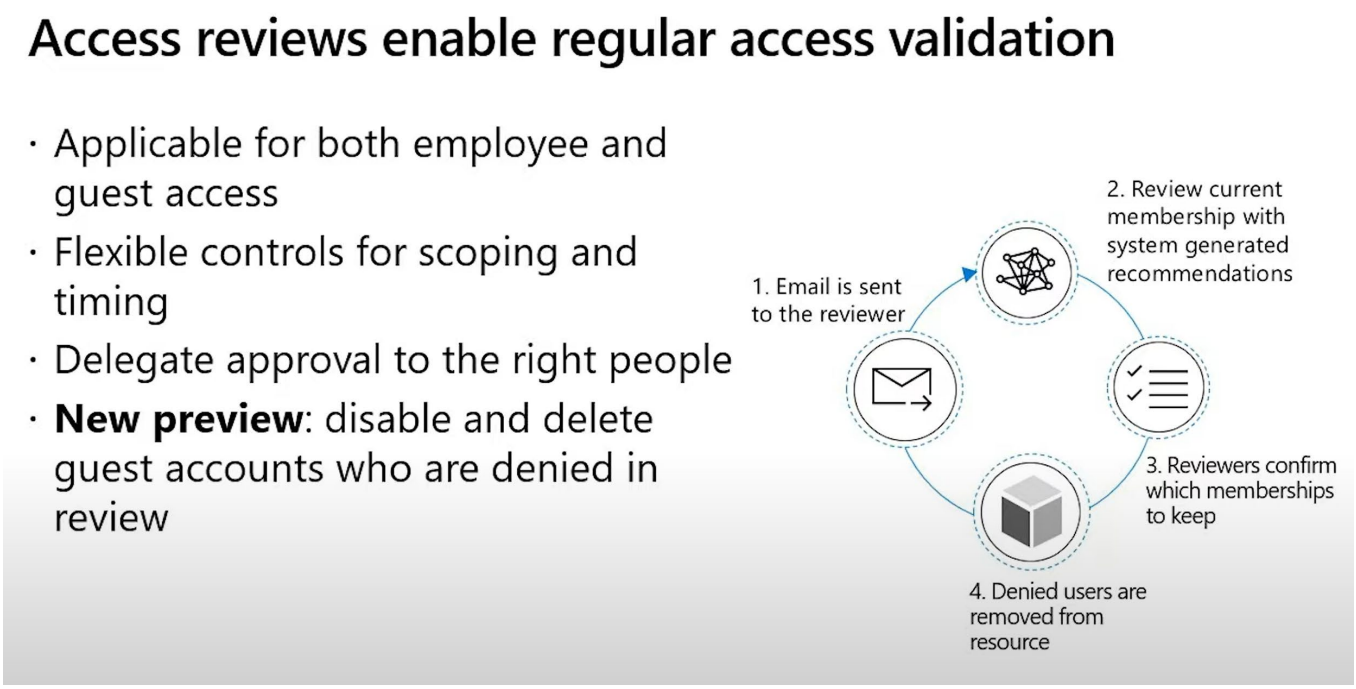
Another approach, more specifically targeted for Access Packages, is to associate a lifecycle policy for the assignment to expire after a given number of days coupled with an Access Review every month or quarter. (We will cover Access Reviews in the next section).



Access Reviews

Azure AD Access Reviews give CDPH the ability to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

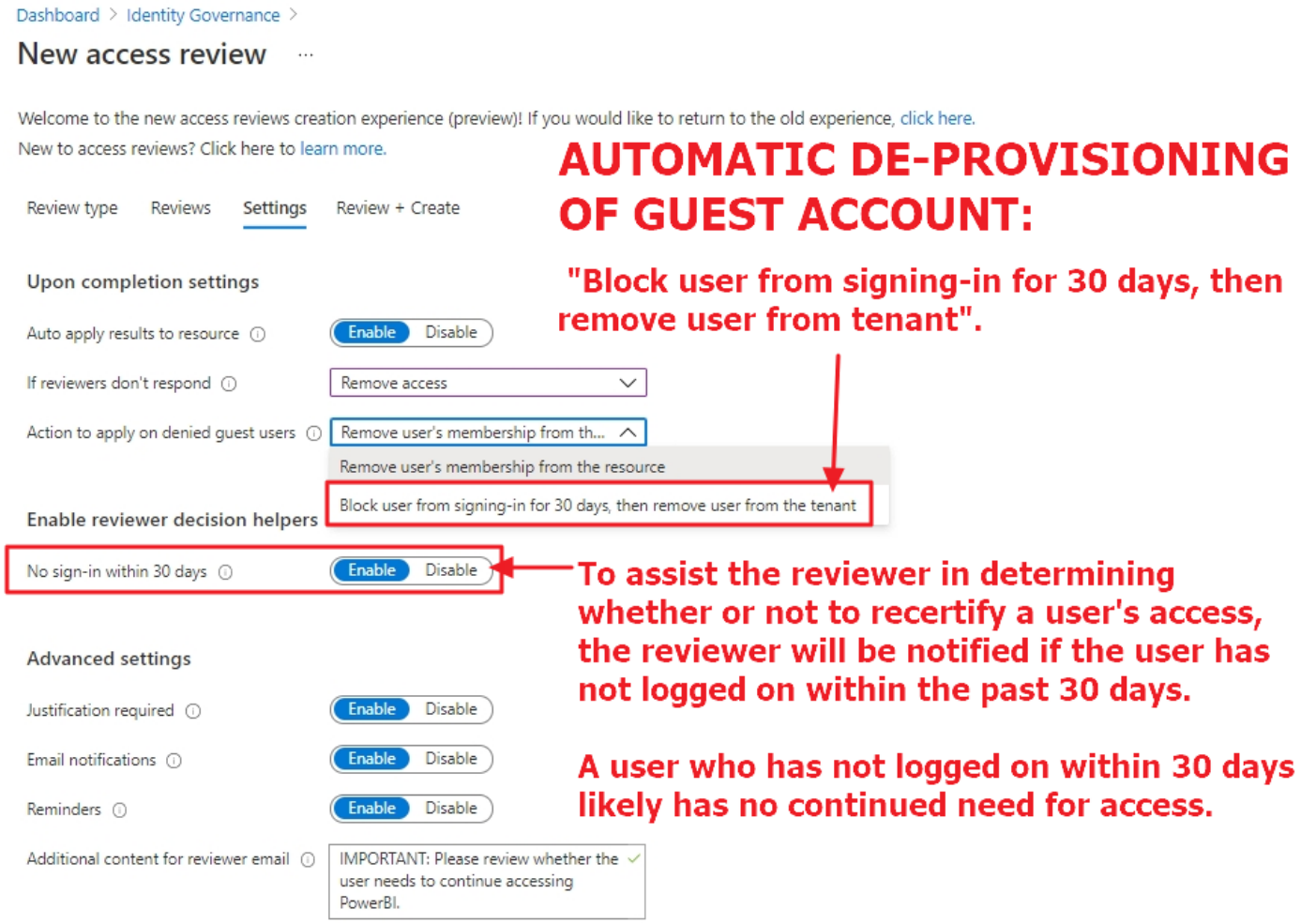
To reduce the risk of stale access, CDPH can enforce a periodic audit and recertification of users who have active assignments to an access package in Azure AD Entitlement Management through Access Reviews.



When creating a new Access Review, in the "Upon completion settings" section, for **Action to apply on denied users** the option **Block users from signing-in for 30 days, then remove user from the tenant**. This setting provides CDPH with the ability to identify, block, and delete external identities from its Azure AD tenant. External identities who are reviewed and denied continued access by the reviewer will be blocked and deleted, irrespective of the resource access or group membership they have.

This setting is best used as a last step after verifying that external users under review no longer carries resource access and can safely be removed from the tenant. The "Disable and delete" feature blocks the external user first, taking away their ability logon and access resources. If there was a mistake or if an IT admin or business unit manager decides to re-enable the user's access, they can do so within 30 days after the user has been disabled. If there is no action taken on the disabled users, they will be deleted from the tenant.

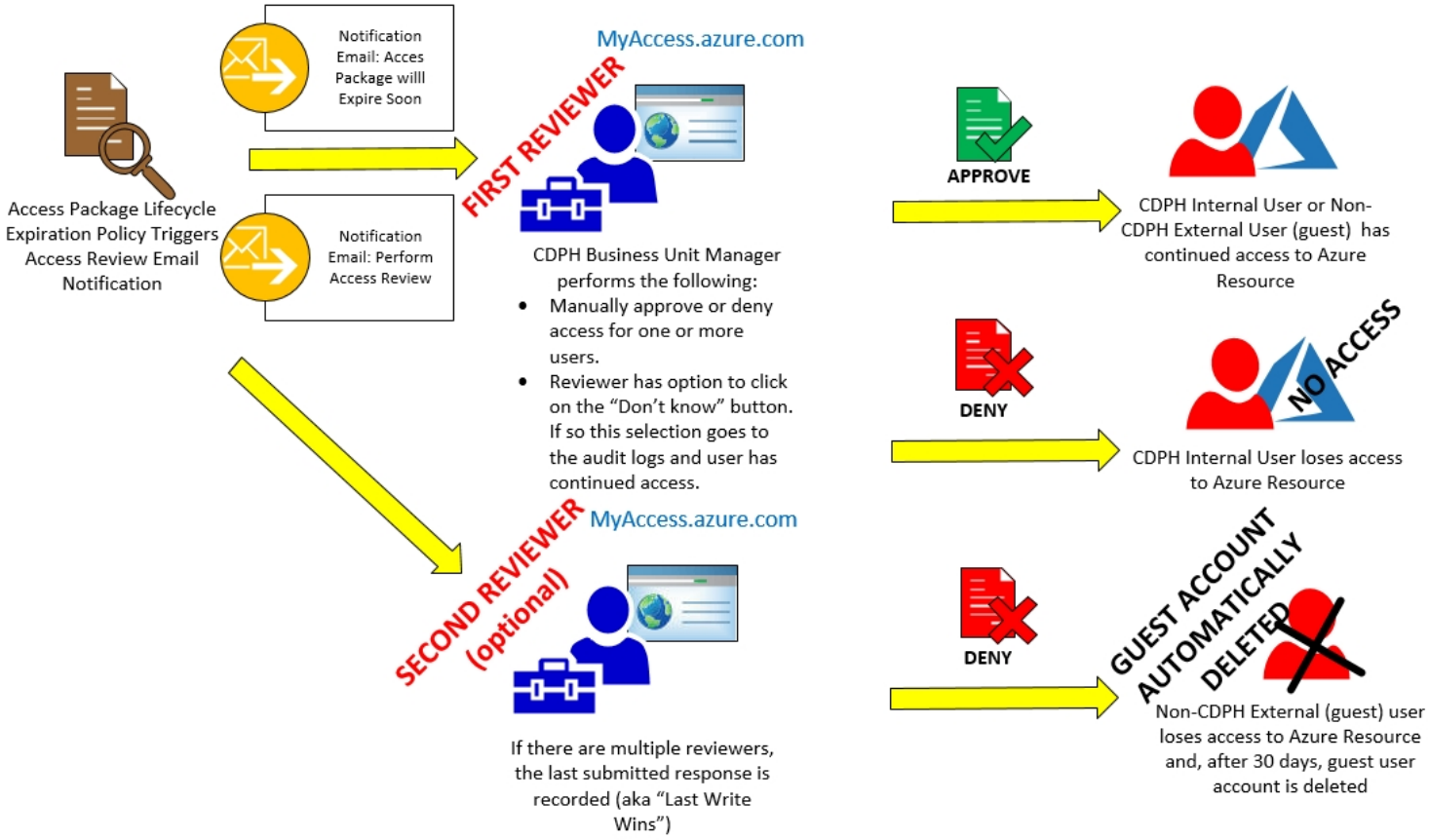
The screen shot below illustrates these options:



The Visio diagram below illustrates the process workflow. The process is triggered automatically by the Access Package's lifecycle policy, which is based on an Access Review conducted either annually, bi-annually, quarterly, or monthly. Next, the primary and / or secondary reviewer performs the review. In the event two reviewers have conflicting responses (eg first reviewer approves and second reviewer denies), the last response recorded is the response that wins out. This is the same as "Last write wins", an old school conflict resolution IT strategy.

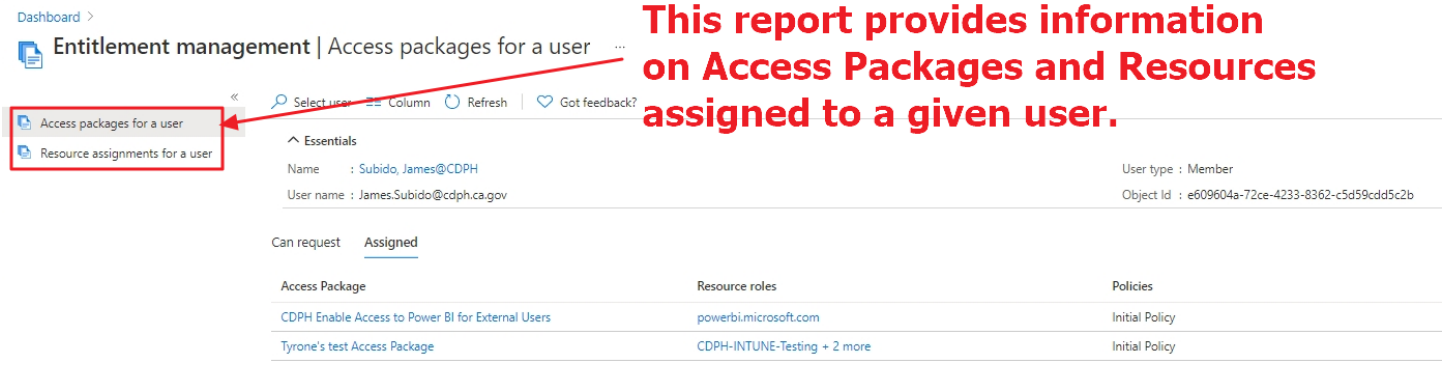
Another role of a secondary reviewer is that in the vent the primary reviewer fails to take action, the Access Review is then forwarded to the secondary (backup) reviewer.

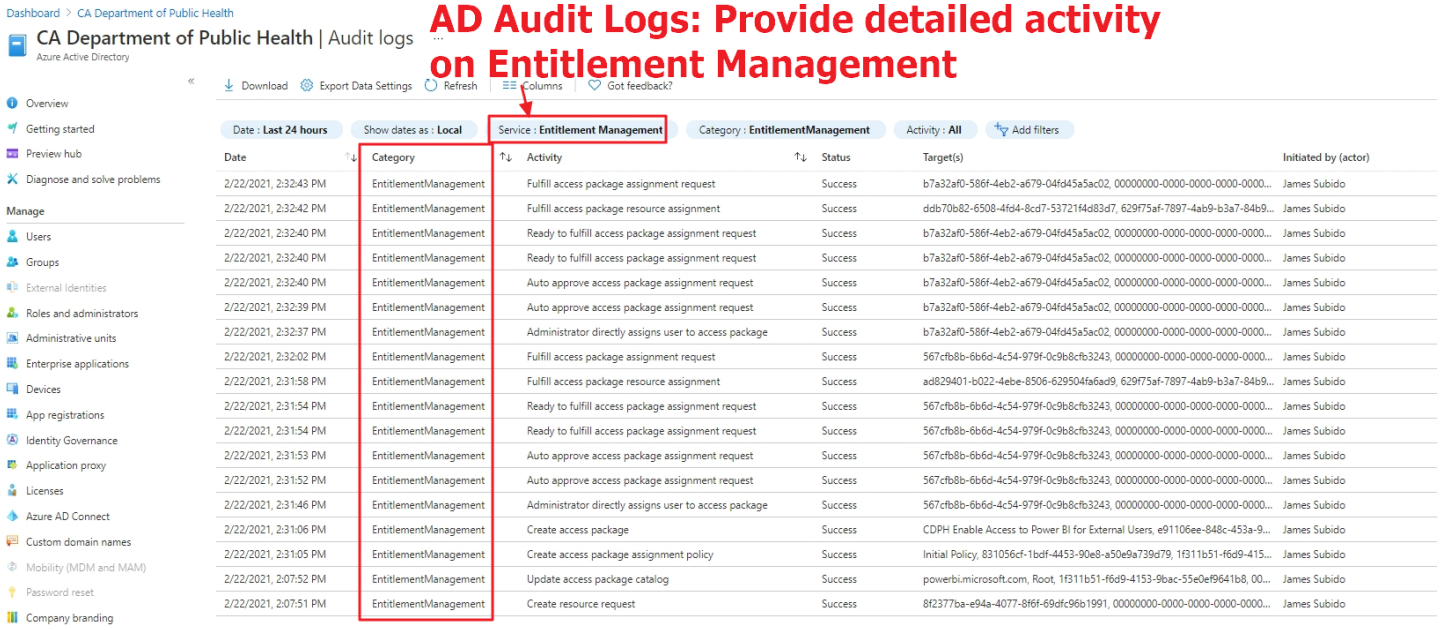
Proposed CDPH Access Review Process



Monitoring Entitlement Management

Entitlement Management provides the following monitoring mechanisms that are user-based (screen shot below), or globally through Azure AD audit logs (second screen shot below):



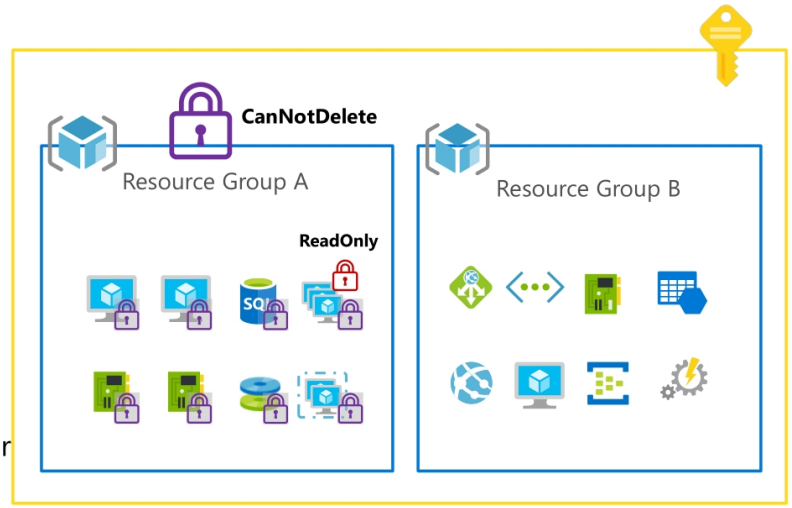


8. Resource Locks

As discussed from a previous section, Azure Role Based Access Control (RBAC) allows CDPH to access resources and define a set of resource actions allowed. RBAC is a first line of defense against unwanted resource access. However, human error is a threat to the integrity of a resource in that an RBAC resource owner may inadvertently delete the resource; consequently, RBAC is not sufficient in such a situation.

Critical Resource Control using Resource Lock

- Prevents Azure Resources from accidental Deletion or Changes
- Current Lock types:
  - ReadOnly
  - CanNotDelete
- Locks are inherited and cumulative
- Can be applied at:
  - Subscription
  - Resource Groups
  - Resource
- Owner and User Access Administrator roles can create and delete Locks

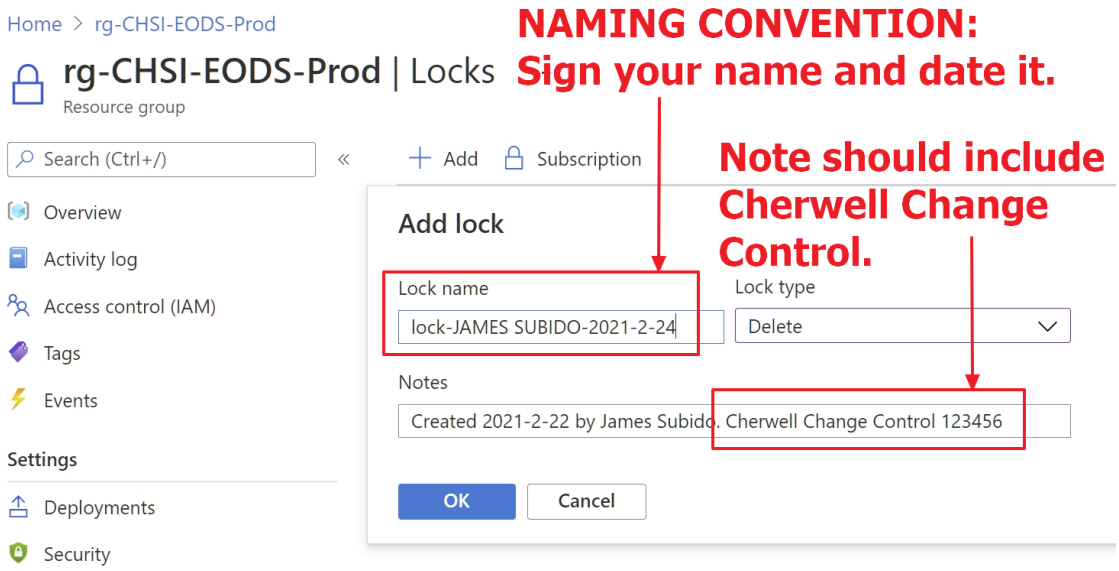


As an additional layer of access control, Azure Resource Locks can be applied to either individual resources, resource groups, or entire subscriptions. When applied at the resource group level, all existing resources as well as any new resources created in the future, will be locked.

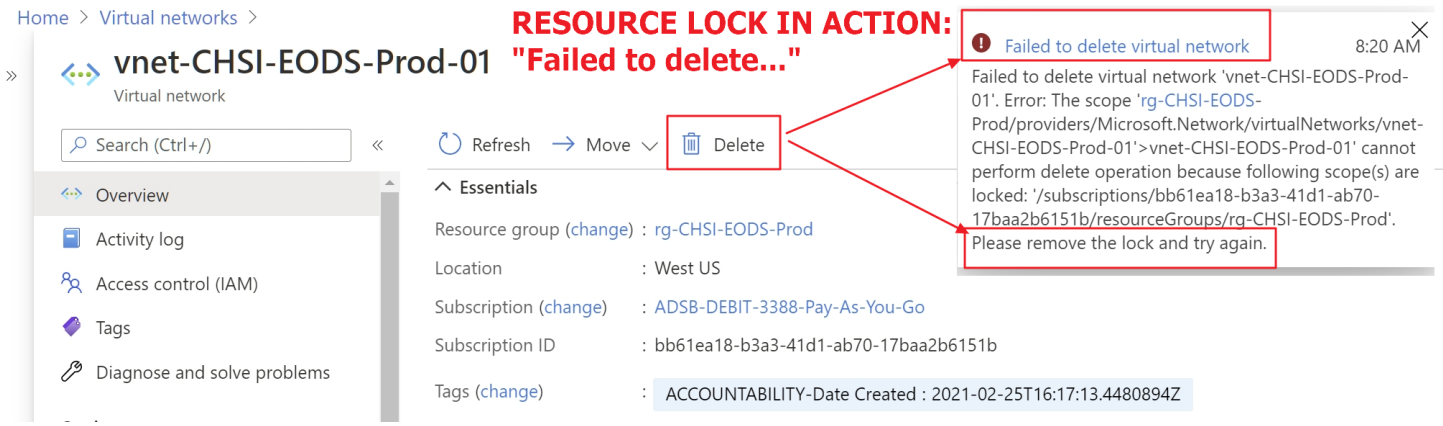
There are two types of resource locks that can be applied:

- **CanNotDelete** – This prevents anyone from deleting a resource whilst the lock is in place, however they may make changes to it.
- **ReadOnly** – As the name suggests, it makes the resource read only, so no changes can be made, and it cannot be deleted.

The naming convention for CDPH's Resource Locks is simple: Simply sign your name and date. In the event a Resource Lock raises questions or if technical issues arise, the owner of the Resource Lock can shed light and / or assist in troubleshooting the issue.



When applied at the Resource Group level, resources within that group automatically inherit the lock. Below is a screen shot of a failed deletion attempt of a Virtual Network:



KEY TAKE-AWAYS:

1) Resource Locks sit outside of the RBAC hierarchy, thus, a user who is an RBAC owner of a locked resource cannot delete said resource.
2) A ReadOnly Resource Lock is more restrictive than a CanNotDelete. When a resource inherits two conflicting policies, the more restrictive policy is enforced.
3) Resource Locks only operate on a resource's management plane. For example, if you were to implement a ReadOnly lock on a SQL Database logical server only prevents you from deleting or modifying the server. Users are still allowed to create, update, or delete data on the databases on that server. These data transactions occur on the data plane.

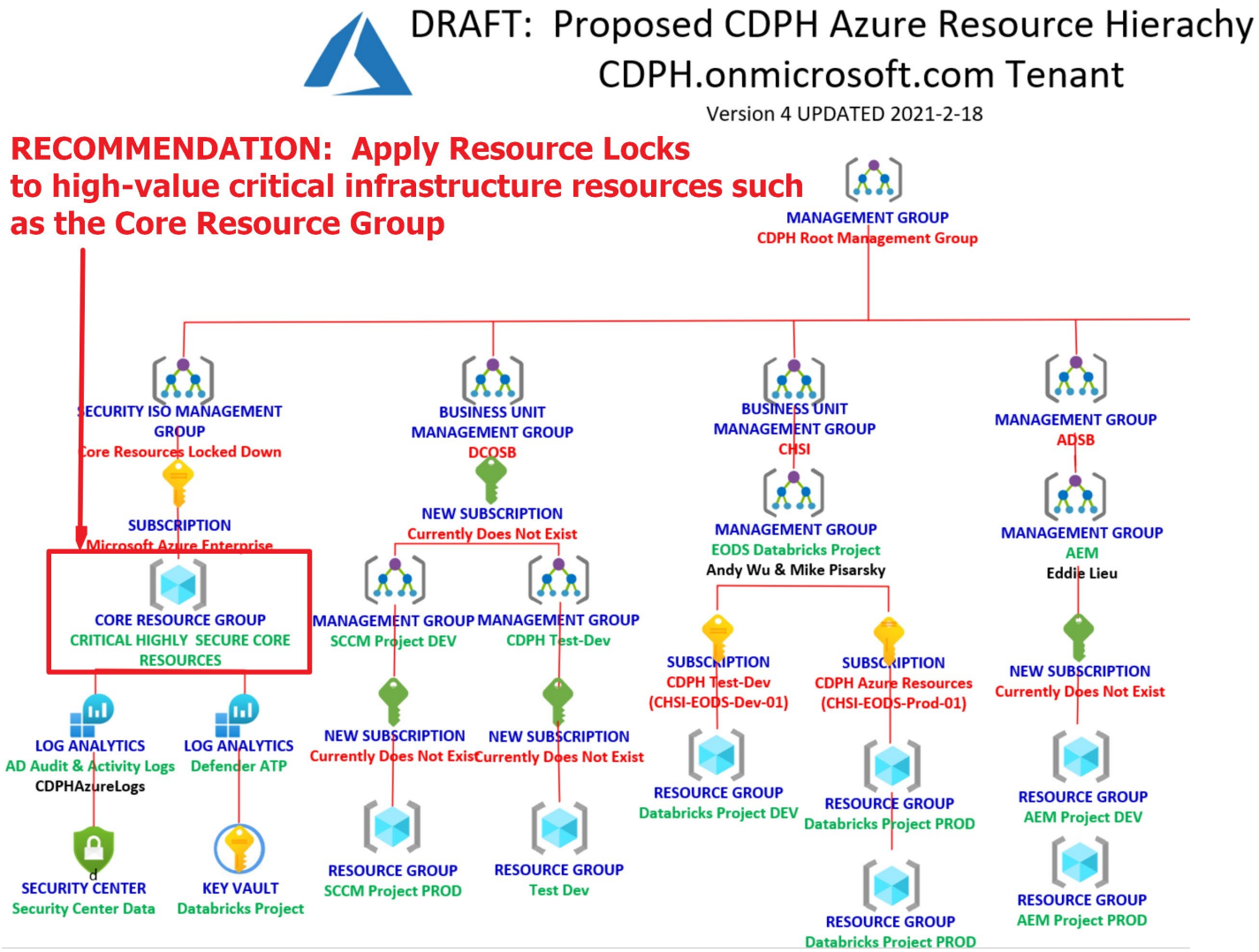
Recommendations for CDPH:

- Use Resource Locks whereever a resource needs to be protected from accidental deletion or modifcation.
- Do not use ReadOnly locks on Storage Accounts (see "Considerations before applhing locks section below).
- Consider implementing the following Resource Locks:

Resource	Scope	Lock
Core resources such as Key Vaults, Storage Accounts, disks, Network Security Groups (NSG), virtual networks, gateways, Network Virtual Appliances (NVAs), to name a few.	Core Resource Group (or possibly Subscription)	CanNotDelete
Production Application' Resources	Resource Group	CanNotDelete
Policies	Resource	CanNotDelete

CHANGE FREEZE: Prevent updates from being applied to certain environments during temporary or critical periods.	Subscription Resource Group Resource	ReadOnly

A Core Resource Group (screen shot below) containing shared infrastructure critical resources is an excellent candidate for a CanNotDelete lock.



GOTCHA: Unexpected results when applying locks can result! Make sure to **read and heed** *"Considerations before applying locks"* below from Microsoft.

REFERENCE: Lock resources to prevent changes - Azure Resource Manager | Microsoft Docs

Considerations before applying locks

Applying locks can lead to unexpected results because some operations that don't seem to modify the resource actually require actions that are blocked by the lock. Locks will prevent any operations that require a POST request to the Azure Resource Manager API. Some common examples of the operations that are blocked by locks are:

- A read-only lock on a **storage account** prevents users from listing the account keys. The Azure Storage List Keys operation is handled through a POST request to protect access to the account keys, which provide complete access to data in the storage account. When a read-only lock is configured for a storage account, users who do not possess the account keys must use Azure AD credentials to access blob or queue data. A read-only lock also prevents the assignment of Azure RBAC roles that are scoped to the storage account or to a data container (blob container or queue).
- A read-only lock on an **App Service** resource prevents Visual Studio Server Explorer from displaying files for the resource because that interaction requires write access.
- A read-only lock on a **resource group** that contains a **virtual machine** prevents all users from starting or restarting the virtual machine. These operations require a POST request.
- A cannot-delete lock on a **resource group** prevents Azure Resource Manager from automatically deleting deployments in the history. If you reach 800 deployments in the history, your deployments will fail.
- A cannot-delete lock on the **resource group** created by **Azure Backup Service** causes backups to fail. The service supports a maximum of 18 restore points. When locked, the backup service can't clean up restore points. For more information, see Frequently asked questions-Back up Azure VMs.
- A read-only lock on a **subscription** prevents **Azure Advisor** from working correctly. Advisor is unable to store the results of its queries.

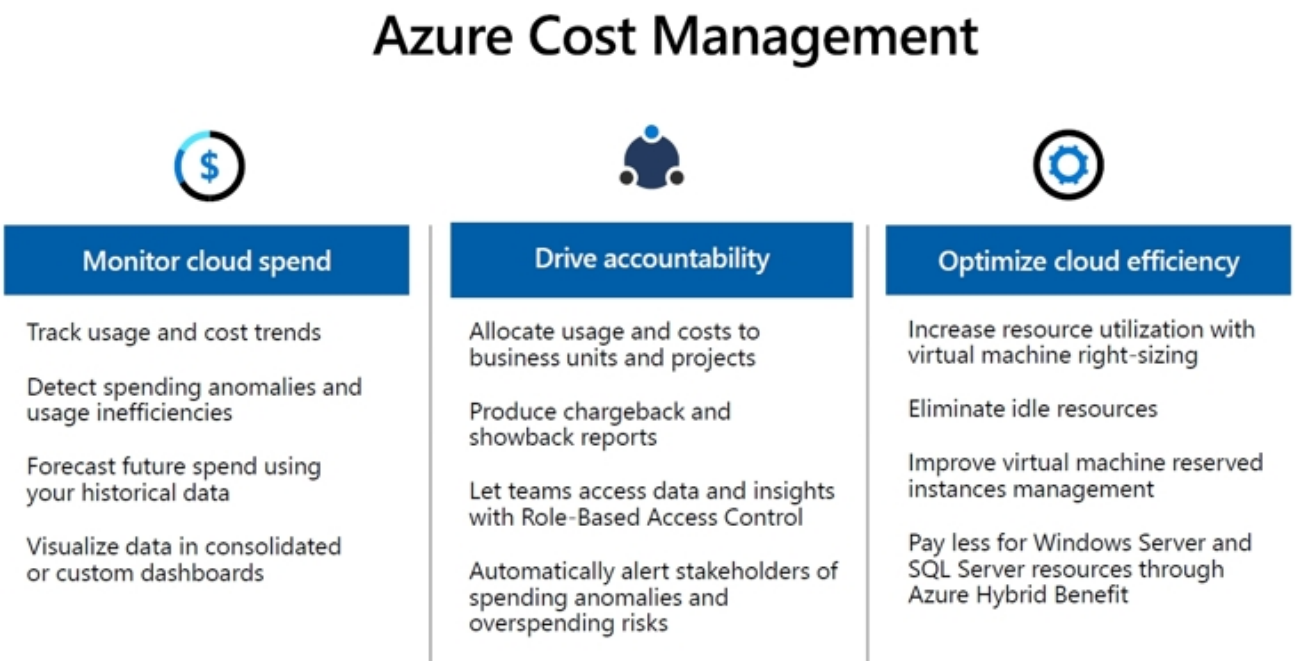
  REFERENCE: Lock resources to prevent changes - Azure Resource Manager | Microsoft Docs

9. Cost Management

"Beware of little expenses. A small leak will sink a great ship."
– Benjamin Franklin

One of the Five Disciplines of Cloud Governance, Cost Management is a concern in the flexible and agile environment of cloud technologies. The deployment of cloud services while addressing the

requirements for performance, unfamiliar new resources, features, and functionality while controlling unpredictable costs can be daunting. This section hopes to provide a process for managing and controlling costs through establishing roles, budgets, accountability.



Unique Subscriptions for Business Unit Managers

The resource hierarchy discussed at the beginning of this document serves as the foundation of CDPH's entire cloud governance framework. Through inheritance, it allows Azure policies and RBAC role assignments to flow down the hierarchy with minimal effort and maintenance. This resource hierarchy will require unique Azure subscriptions to sit in between business unit management groups and the resource groups that contain the resources and services CDPH will consume.

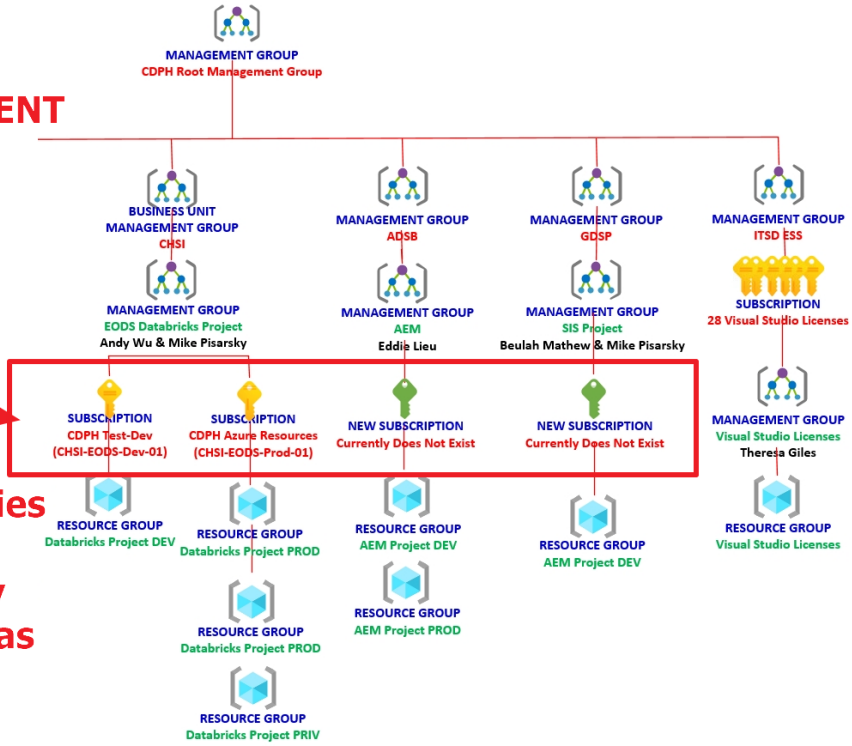
This allocation of unique Azure subscriptions to business unit managers is the key to establishing their role in cost management accountability. A unique subscription would empower them to establish budgets, develop alerting measures through email and SMS text, generate reports, receive optimization advice, and proactively address forecasted costs based on existing estblished utilization patterns.

The screen shot below illustrates how the subscriptions are tied to each business unit manager's management group which will then tie in to the Azure resources and services they own and consume.

CDPH's COST MANAGEMENT STRATEGY:

Key to this strategy is providing Business Units with their own subscription.

Key to being able to deploy Governance Policies to Business Unit Management Groups rely on unique subscriptions as well.



GOTCHA: Subscription-based Cost Management has compelling advantages over Resource Tag-based Cost Management due to the latter's limitations:

> *"Most Azure resources support tagging. However, **some tags are not available in Cost Management and billing**. Additionally, **resource group tags are not supported**. **Support for tags applies to usage reported after the tag was applied to the resource.** Tags aren't applied retroactively for cost rollups."*

REFERENCE: Quickstart - Explore Azure costs with cost analysis | Microsoft Docs

Cost Management Capabilities

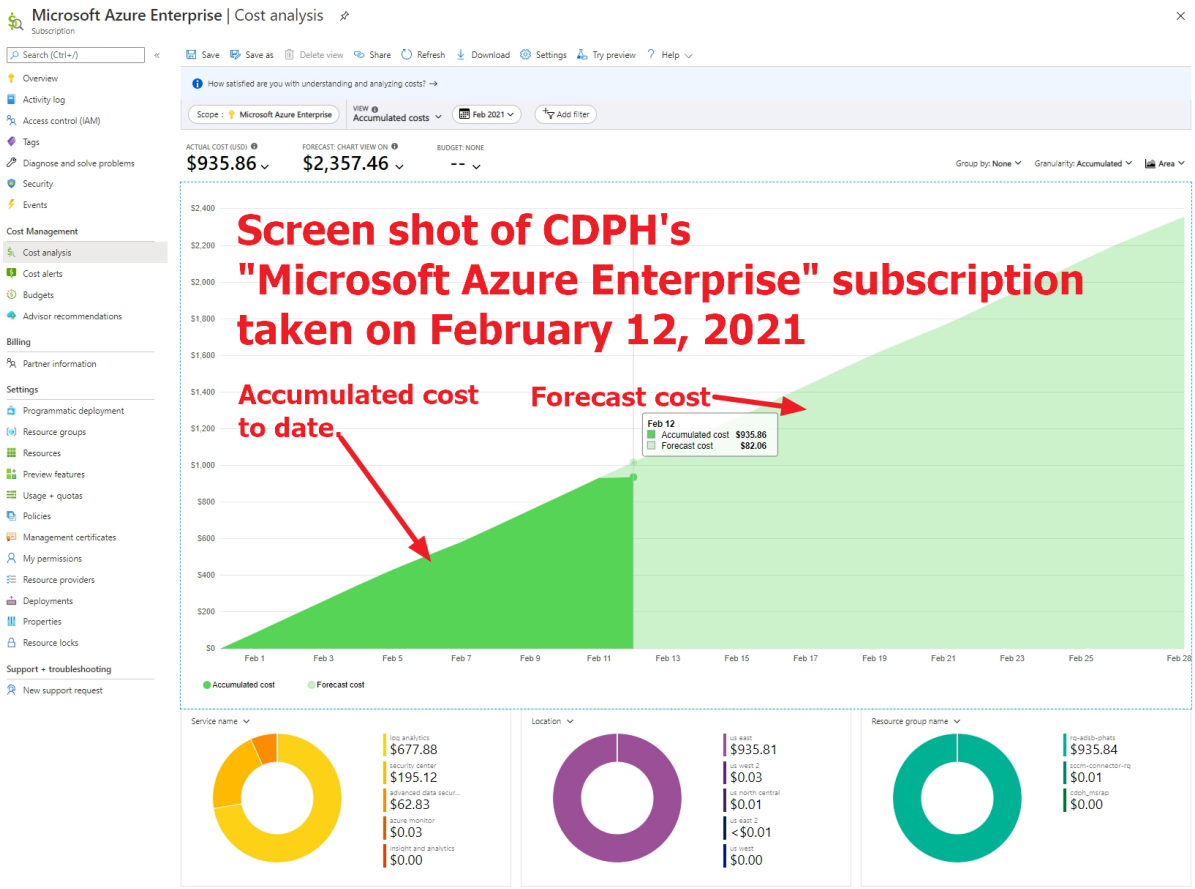
When logging in to the Azure Portal, Cost Management is a native tool that is enabled by default. It provides detailed costs analysis and filtering capabilities that leverage resource tags (discussed earlier). It provides the business unit manager with the ability to establish a budget, allocate costs, establish notification, among others.

Cost Analysis

The cost analysis view provides detailed cost exploration with a lot of functionality. A breakdown of costs by resource type and resource group name will pinpoint which Azure services are incurring most of the costs. Other capabilities include:

- Group, filter and view using 18 dimensions such as tag name, resource type, etc.
- Built-in and custom date ranges.
- Budget integration and alerting based on exceeded thresholds

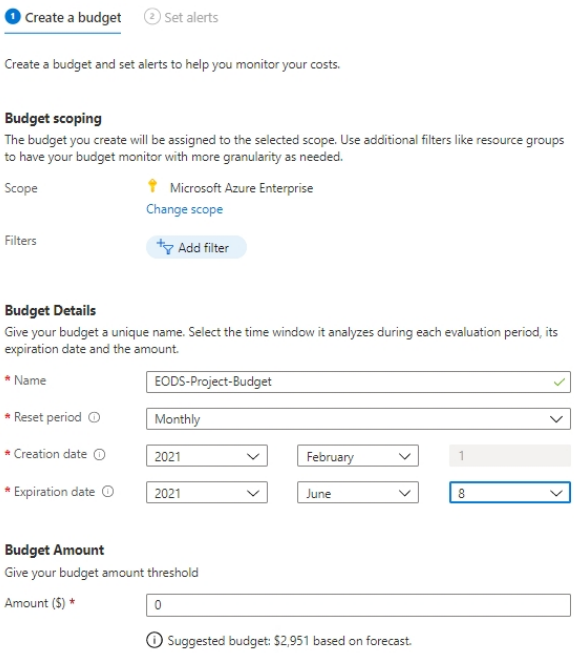
Here is a screen shot of the cost analysis screen which provides information on current cost as well as a forecast based on existing utilization:

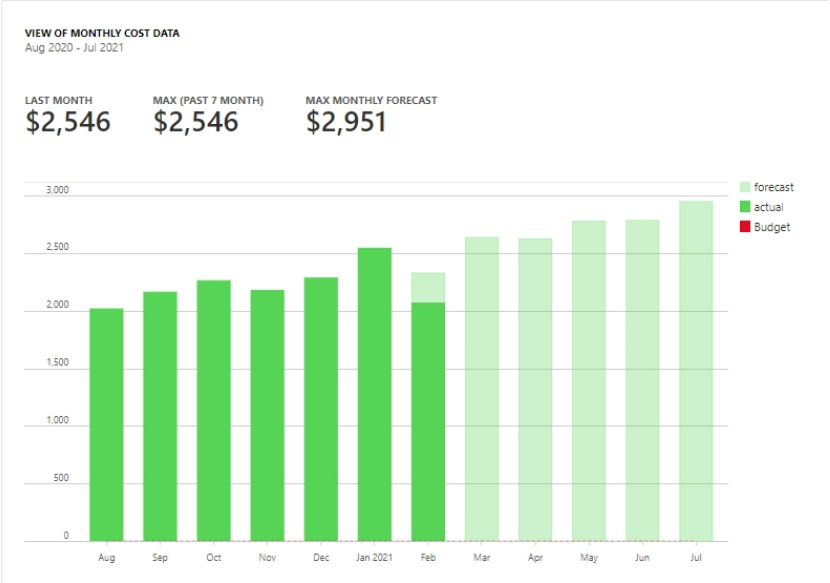


Budgets

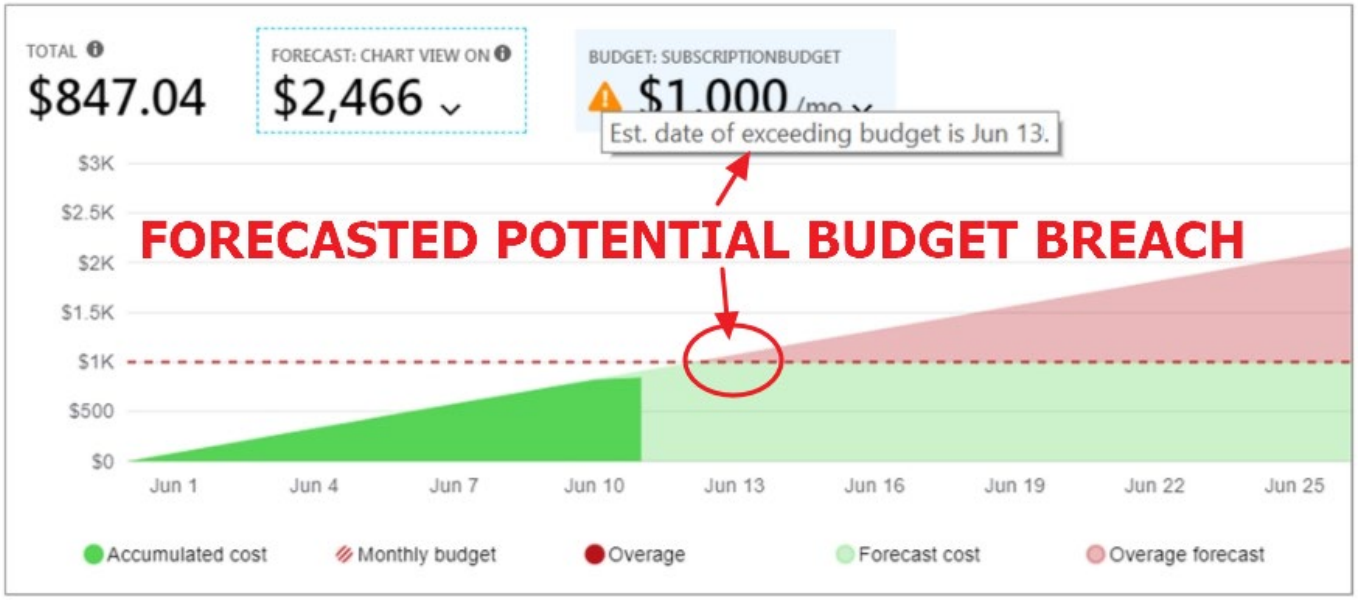
Budgets are the key mechanism for preventing unexpected spending. Azure budgets can be created on three levels: 1) management group; 2) subscription; or 3) resource group. The business unit manager can track cumulative Azure spending, in which case the budget is scoped at the subscription level or based on specific programs – which will require management group-based budgets.

A budget can be created within a few minutes with historical spending data to help guide you in its establishment. Here is a screen shot of the budget creation screen:



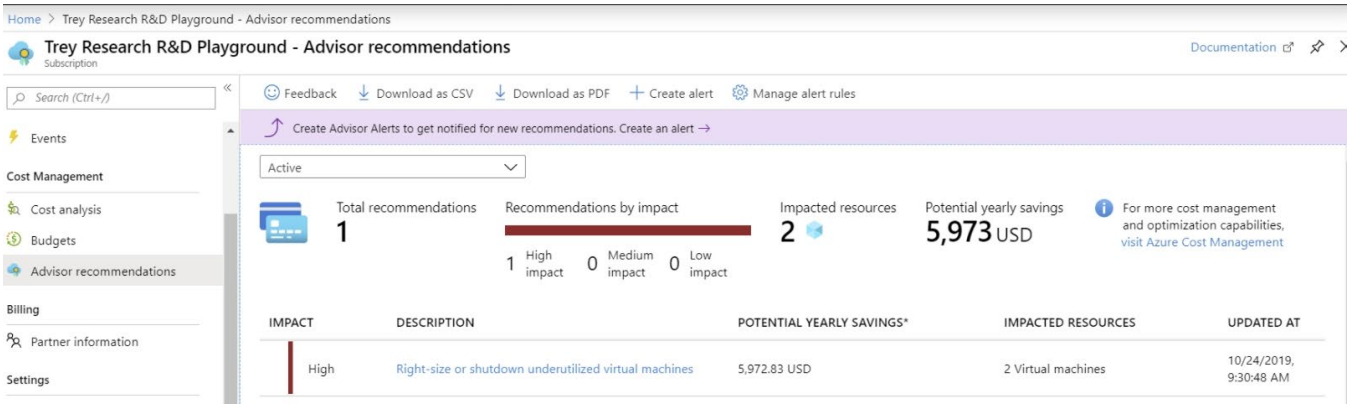


Once a budget is defined, alerting can be established to generate notifications on specific consumption thresholds you establish.



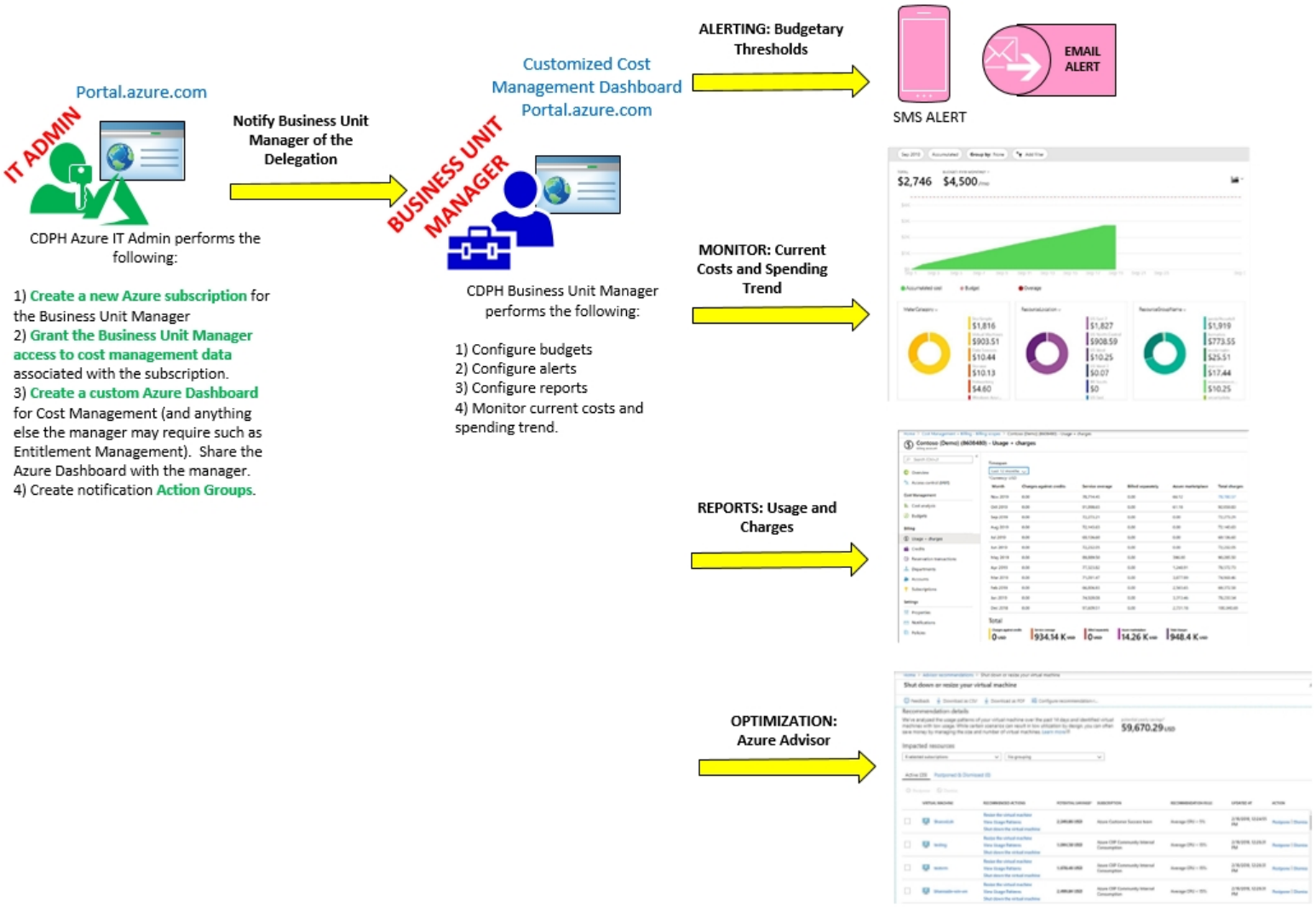
Cost Optimization with Azure Advisor

Azure Advisor is a free governance tool that provides best practice recommendations for several areas. Within the context of Cost Management, it makes specific cost savings recommendations based on usage and configurations.

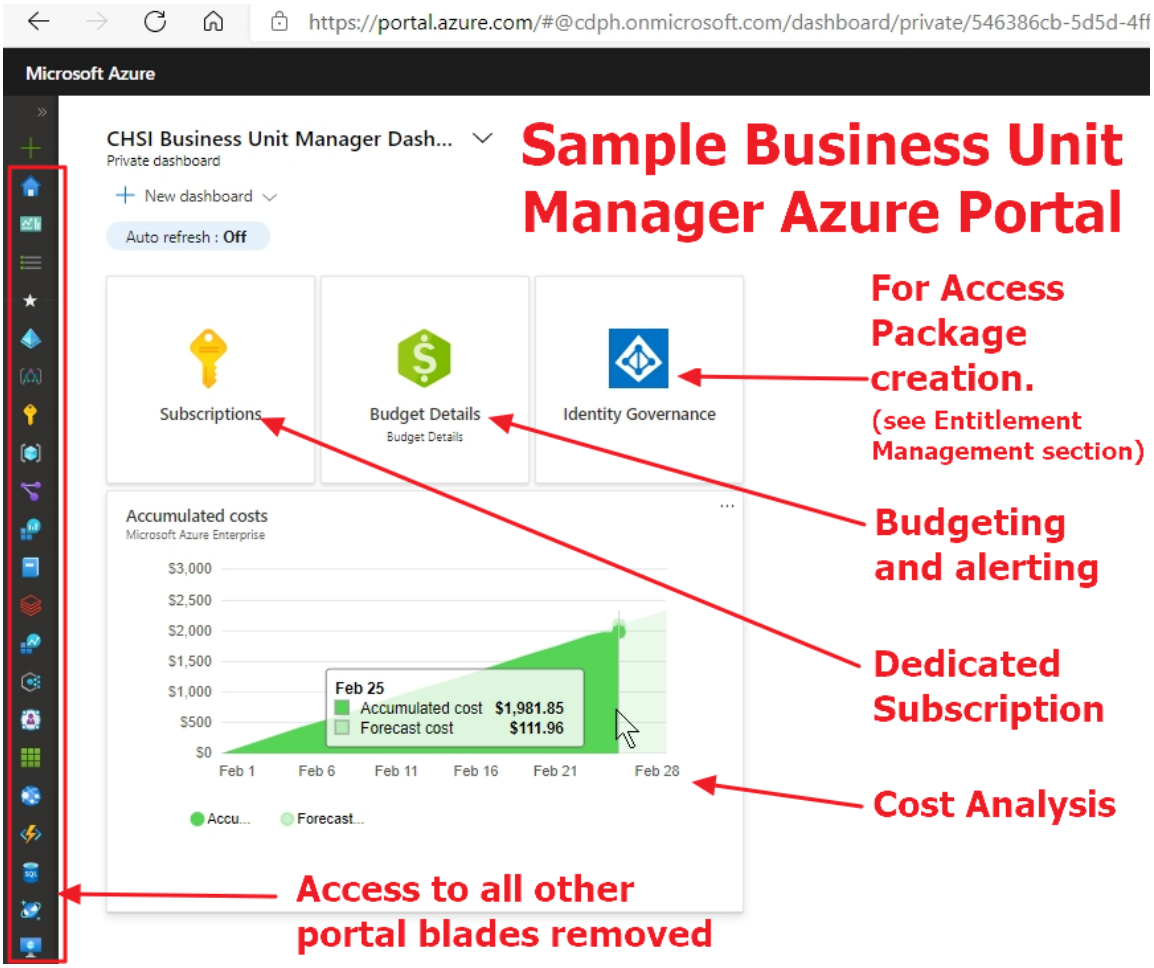


The process below establishes the process of setting up a business unit manager to access Azure Cost Management and activities the manager will perform in order to manage costs. Note that the manager will require Cost Management Contributor RBAC role in order to perform the tasks shown.

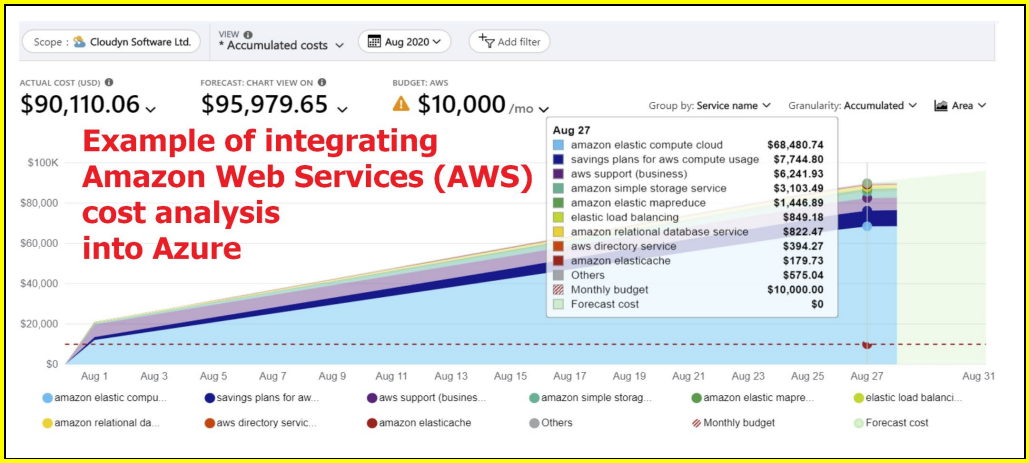
Proposed CDPH Cost Management Process



The screen shot below shows the custom dashboard for the business unit manager's use. It includes only those elements required for cost management. A component called Identity Governance is an optional component to allow the manager to generate access packages (discussed in a previous section).



TIP: Since CDPH maintains an AWS presence, Azure Cost Management has the ability to integrate Amazon Web Services (AWS) costs and usage information as shown here:

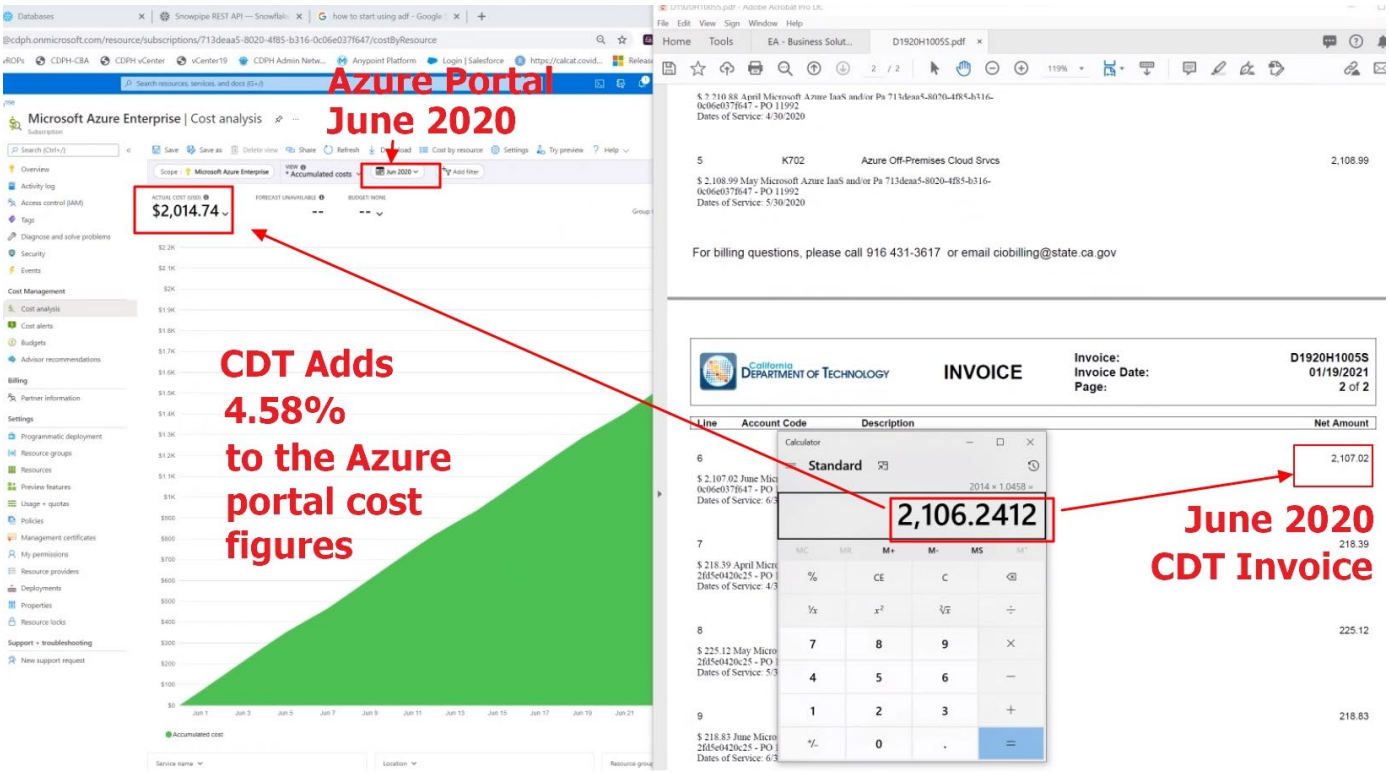


REFERENCE: [Manage AWS costs and usage in Azure Cost Management | Microsoft Docs]

California Department of Technology (CDT) Invoicing

Microsoft's Azure invoices are billed through California Department of Technology (CDT) which adds a charge on top of Microsoft's rates. The process of reconciling these CDT invoices with the charges

presented on the Azure Cost Management portal requires adding 4.58% to the charges on the Azure Cost Management portal to match the CDT invoice as shown in the screen shot example below:



On the left of the screen shot is the Azure Cost Management Portal reflecting a charge of $2,014.74. Adding 4.58% brings us to the figure shown in CDT's invoice for June 2020 (shown on the right side of the screen shot).

OBSERVATIONS ON THE CDT INVOICE:

- The invoice presents individual line items in the form of aggregated charges per subscription per month.
- The subscription is addressed using the GUID ID name 713deaa5-8020-4f85-b316-0c06e037f647 instead of the friendly name. Perhaps this is something we can bring up to CDT for remediation.

10. Blueprints

"Build it right with guardrails and continually update the guardrails as requirements change." -- JS

As CDPH's very busy ITSD architecture unit is a small team that quickly becomes a bottleneck for deploying new Azure resources, Azure Blueprints are a custom orchestration engine for stamping out new environments with governance from the onset. In other words, CDPH can take its architecture team's knowledge and guidance and package them into a Blueprint.

A Blueprint is a repeatable template that CDPH's architecture team defines once and then deploys during the creation of new management groups and subscriptions. This allows CDPH to define its governance through RBAC and policies then encapsulate them into a Blueprint for rapid deployment to stand up new fully governed environments. Additionally, changes to Blueprints can be tested prior to production deployment using version control (more on this later).

Blueprint Definitions

Blueprint definitions Azure blueprints are defined by so-called artifacts. An artifact can currently be one of the following:

- **Resource group:** A resource group that is created by a Blueprint can be used by other artifacts within the scope of the Blueprint. For example, you can create a resource group in a Blueprint and then reference an ARM template to this new resource group.

- **Policy/Initiative Assignments:** You can assign an existing policy to a subscription or resource group that a Blueprint is assigned to. For example, you can assign the "CDPH-Tag resource with Owner Name and Date policy".

- **RBAC Role assignments:** You can assign management access to management group based on group membership. For example, users who are a member of the rbac-CHSI-EODS-Prod-01-mg-Contributor Azure AD group are given contributor rights.

- **Azure Resource Manager templates:** With an ARM template, CDPH's ITSD administrators can declaratively deploy complex Azure environments. ARM templates can be used within the scope of Blueprints. For example, automatically create a new Log Analytics workspace in a resource group that is created within the scope of a Blueprint.

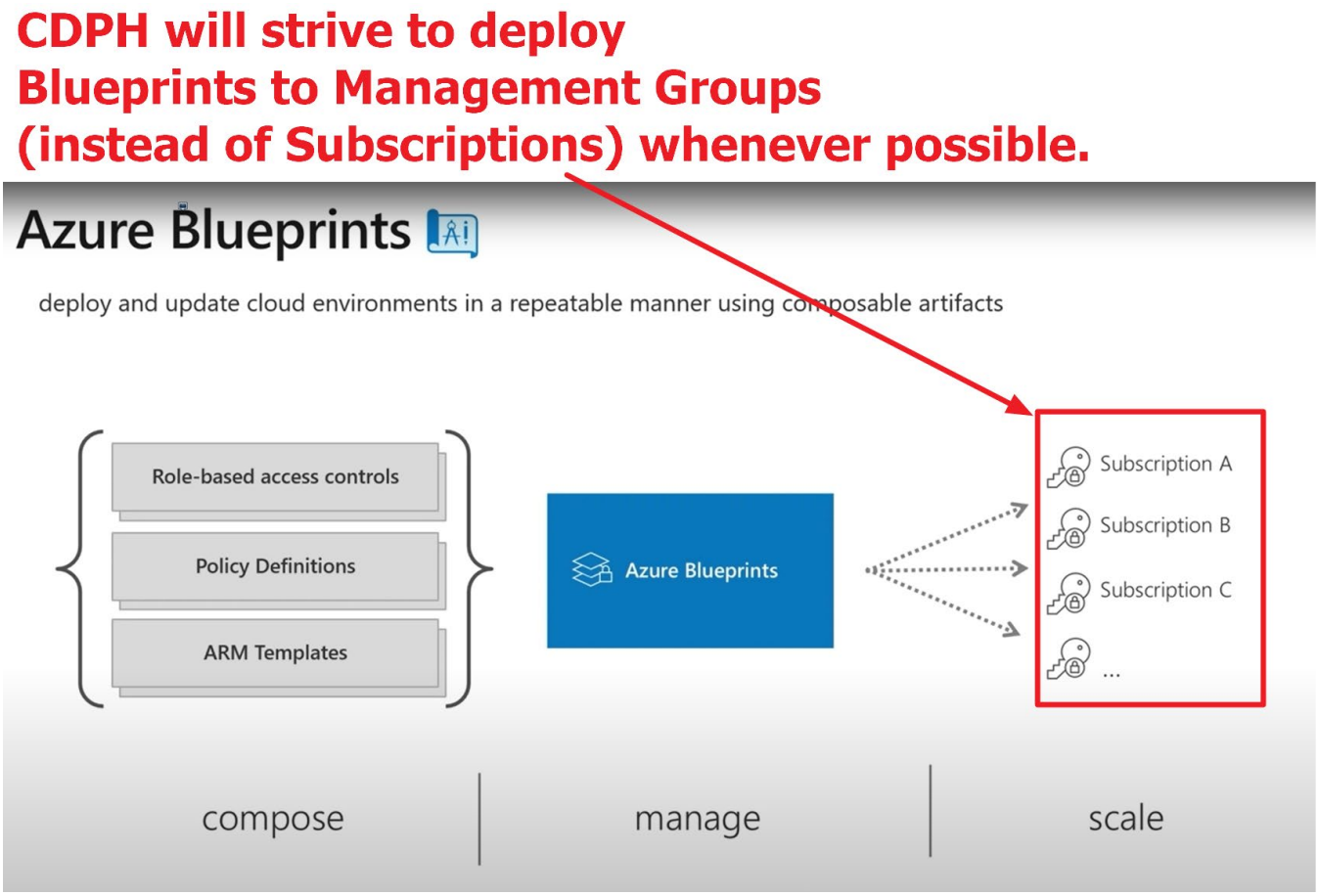
It is important to note that all of the above artifacts must be created before you define a Blueprint which will contain them.

GOTCHA: Once a Blueprint definition location is located and saved, it cannot be changed. The best practice recommendation is to save all Blueprints in the CDPH Root Management

Group for deployment across all child management groups in CDPH's entire resource hierarchy.

Blueprint Publishing and Assignment

All new Blueprints are designated in a draft state; they cannot be deployed (Azure calls it "assigned") in that state. You must first publish the Blueprint, which requires you to provide a version and (optionally) notes. The version must be a string that can contain letters, numbers, and hyphens with a maximum length of 20 characters. Changes to a published blueprint require a new version and (optionally) notes that you can use to document the changes.



Each published version of a Blueprint can be assigned to an existing management group or subscription. The recommended practice is to assign Blueprints to management groups (associated with business units that persist) instead of subscriptions (which have a limited lifecycle). In the portal, the Blueprint defaults the version to the one published most recently. If there are artifact parameters or blueprint parameters, then the parameters are defined during the assignment process.

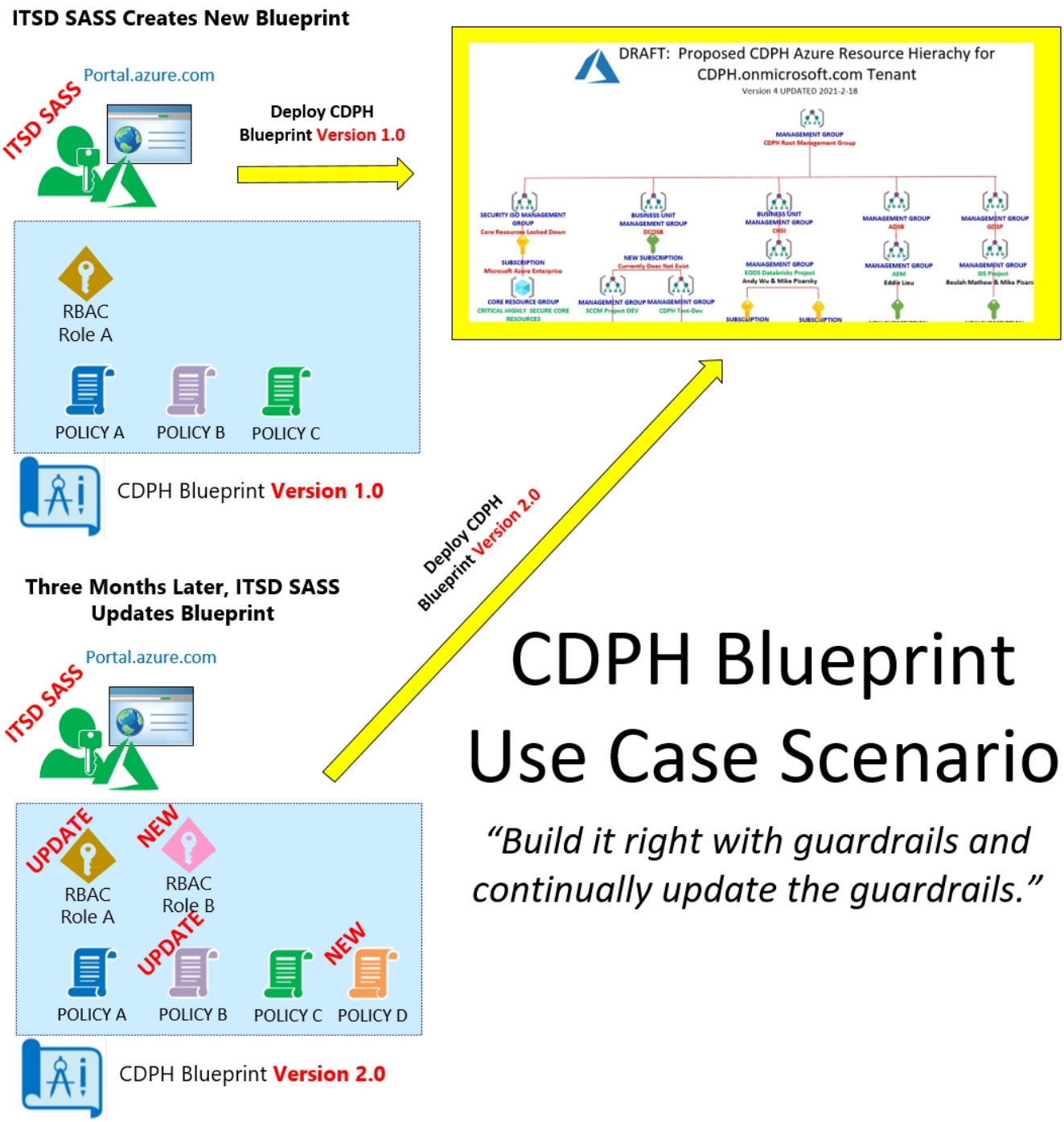
(NOTE: Please see *Chapter 7: Naming Conventions* for guidance on how to name blueprints, assignments, and versions).

NOTE: Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the Create Or Update REST API must be used and the request body must include a value for *properties.scope* to define the target subscription.

REFERENCE: Overview of Azure Blueprints - Azure Blueprints | Microsoft Docs

CDPH Use Case Scenario

Bringing together all the elements of Blueprints from the previous sections, here is a sample process flow that involves a Blueprint with one custom RBAC role called Role A and three policies. The Blueprint is published and assigned to CDPH's management group hierarchy at the root level. Three months later, CDPH's ISO department mandates changes to the Blueprint -- a second custom RBAC role needs to be created and updates need to be performed on the existing RBAC Role A and Policy B. These changes necessitate a versioning update to version 2.0 since version 1.0 can no longer be updated as it has already been published. The changes are performed to version 2 and published to the CDPH Root Management Group. The Visio diagram below illustrates this process:



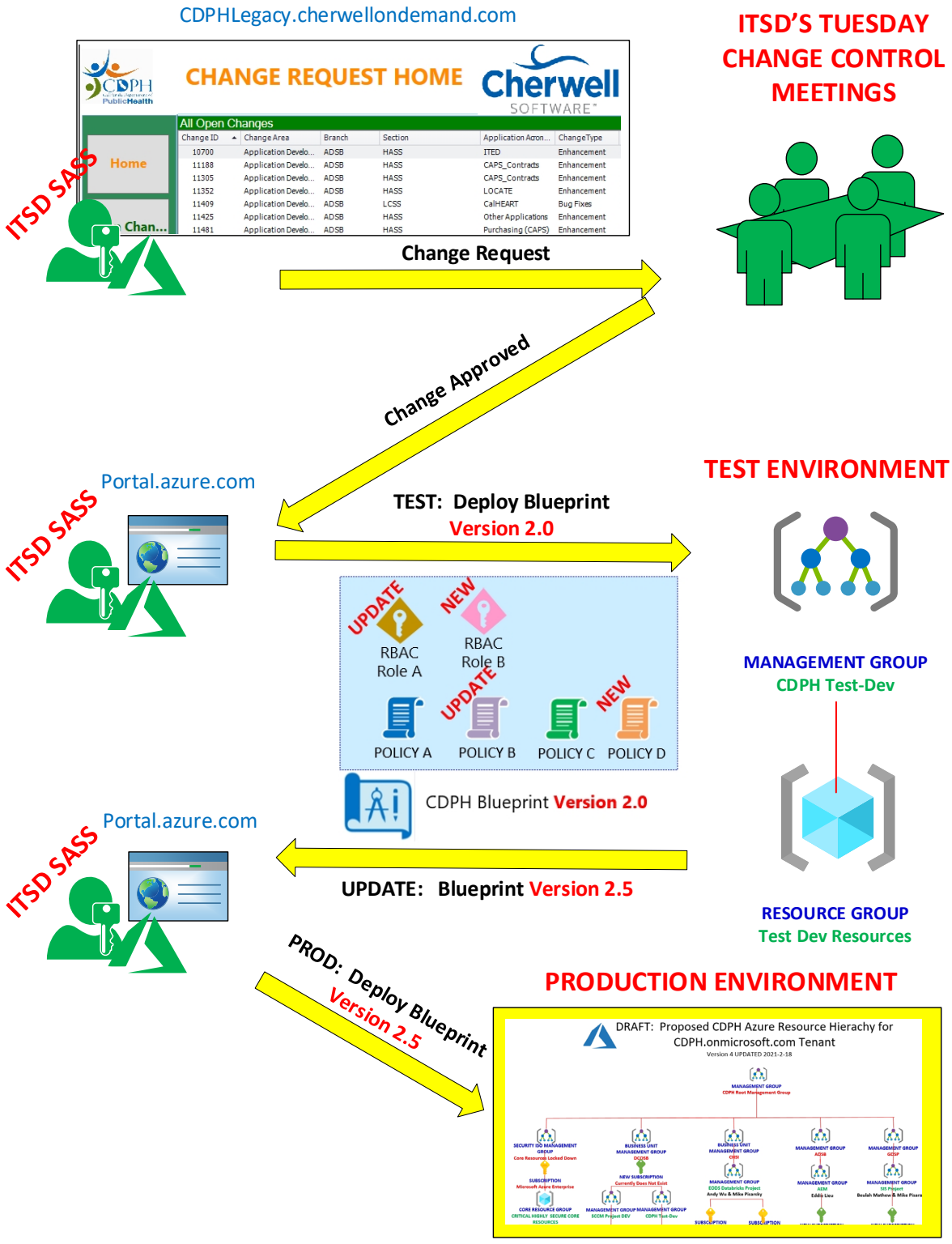
Integrating Blueprint Version Control into CDPH's Change Control Process

Note that the Visio diagram above is a simplified diagram that omits the change control process. The key take-away with Blueprint versions is that since can have multiple versions of a given Blueprint, this allows CDPH the ability independently assign each Blueprint version to a different management group, thus allowing the process to comply with CDPH's established change control process which requires a Cherwell Change Request approval process followed by a development and testing prior to production deployment.

The Visio diagram below highlights the process flow just described. The goal of this process flow is to deploy updates to the CDPH Blueprint version 1.0 as discussed in the preceding section. The updated Blueprint will carry the version 2.0 designation the details of which comprise the scope of the Cherwell Change Request. Note that because testing and development is an iterative process, incremental changes to version 2.0 revealed during testing necessitate a revision to version 2.5, which is the final version deployed to the CDPH production environment.

Since key to any deployment plan is an effective and reliable rollback plan to prevent RGEs (Resume Generating Events), the backout plan to any Blueprint deployment is simply to revert to the previous version which in this example is version 1.0.

Blueprint Version Control with CDPH Change Control

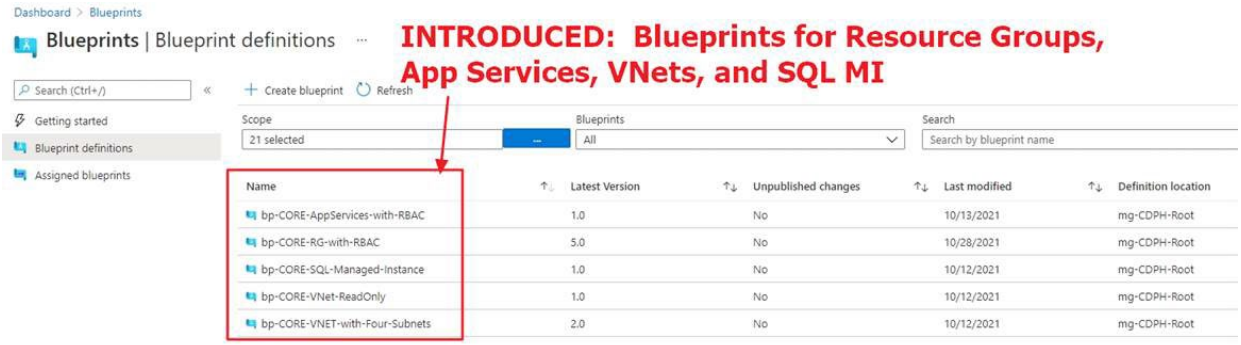


CDPH Action Item on Blueprints

The recommended approach is for CDPH to first develop the recommended resource hierarchy discussed at the beginning of this document. Next, the Azure policies and initiatives and RBAC role assignments need to be defined, validated, and deployed. (Due to the diverse Azure resource requirements of business units, the use of ARM templates may not be a realistic fit at this time).

Once CDPH has a firm grasp on policies, initiatives, and RBAC role assignments, only then might it be suitable for the development of Blueprints.

UPDATE: December 15, 2021: Introduced Blueprints for GDSP SIS v2.0 project deployment.

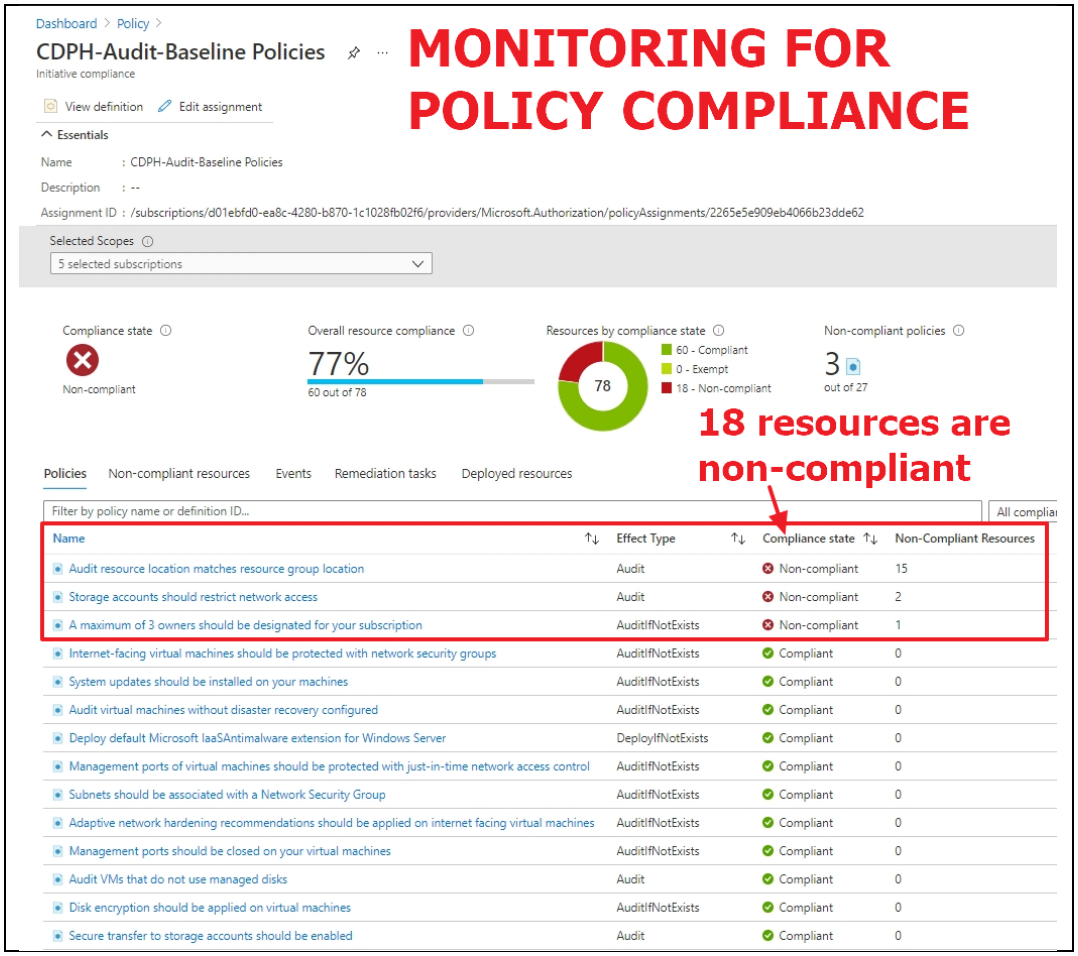


11. Monitoring for Compliance and Changes

Once CDPH's Azure governance framework is in place, the next step is to monitor the environment for compliance of policies, initiatives, and blueprints. Additionally, the ability to detect and understand changes to resources either from an individual or by an automated process is also important.

Azure Resource Compliance

Azure Policy generates data that provides an insight on the compliance state of CDPH's environment. As we discussed *in Chapter 9: Policies*, the Azure policies and initiatives provide control in many ways, such as ensuring that resource tags for ownership and creation date are stamped on resources as well as ensuring that CDPH's resources are only created in the West US region. Any violations to these policies are flagged through data provided by Azure Policy as shown in the following screen shot:



We show 18 resources as non-compliant for three policies, all of which are in audit mode as opposed to enforced. Audit mode allows us to determine the impact of the policy to the environment before we enforce it.

Compliance Evaluation Frequency

Evaluations of assigned policies and initiatives happen as the result of various events:

COMPLIANCE EVALUTION FREQUENCY:

- New or updated policy = 30 minutes
- New or updated resource = 15 minutes
- Policy exemption = (determination in progress)
- Periodic Cadence = 24 hours
- On-demand evaluation scan = 15 minutes

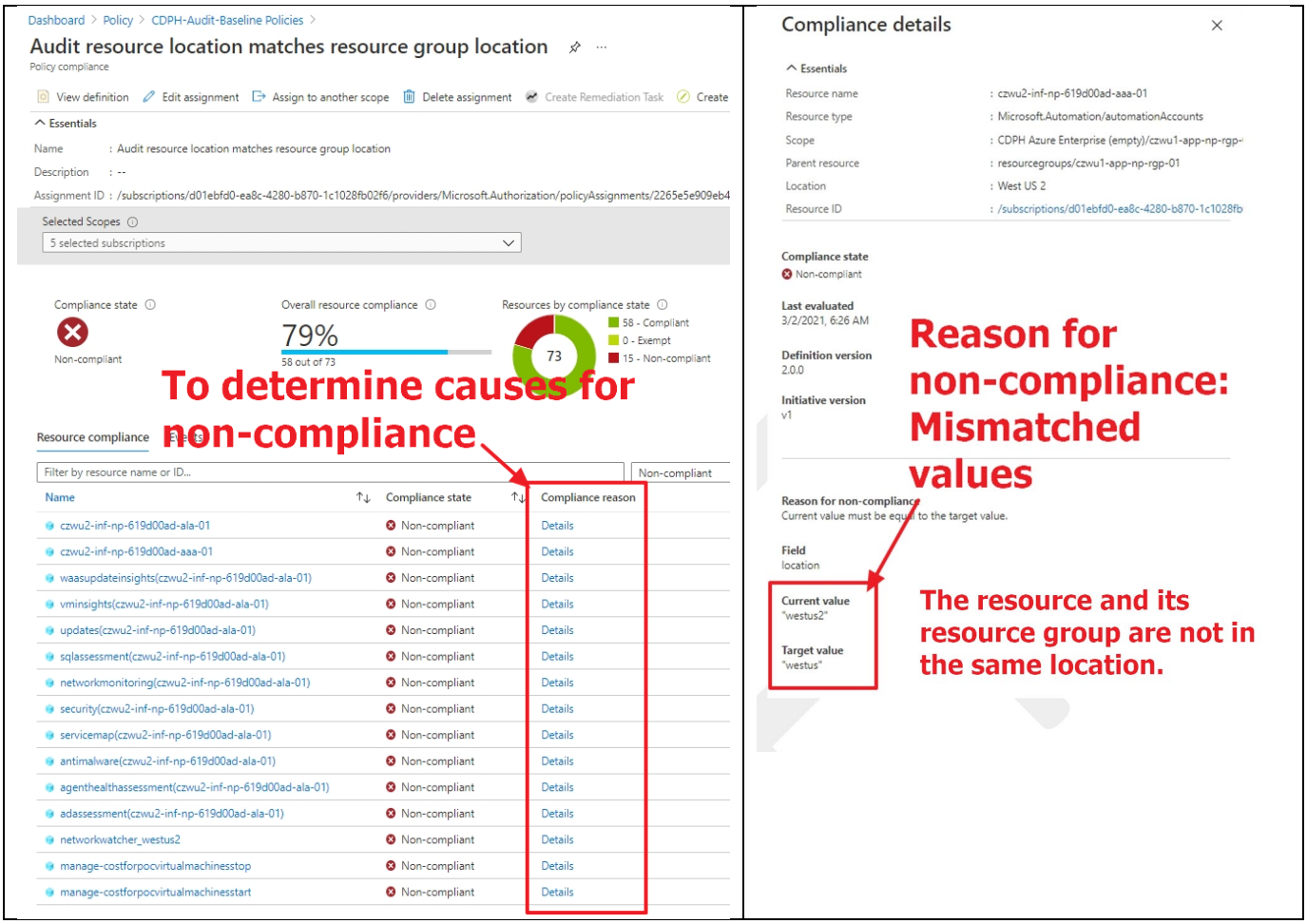
- NEW POLICY: A policy or initiative is newly assigned to a scope. It takes around **30 minutes** for the assignment to be applied to the defined scope. Once it is applied, the evaluation cycle begins for resources within that scope against the newly assigned policy or initiative and depending on the effects used by the policy or initiative, resources are marked as compliant, non-compliant, or exempt.
- UPDATE POLICY: A policy or initiative already assigned to a scope is updated. The evaluation cycle and timing for this scenario is the same as for a new assignment to a scope, which is **30 minutes**.
- NEW OR UPDATED RESOUCE: A resource is deployed to or updated within a scope with an assignment via Azure Resource Manager, REST API, or a supported SDK. In this scenario, the effect event (append, audit, deny, deploy) and compliant status information for the individual resource becomes available in the portal and SDKs around **15 minutes** later. This event does not cause an evaluation of other resources.
- POLICY EXEMPTION is created, updated, or deleted. In this scenario, the corresponding assignment is evaluated for the defined exemption scope.
- PERIODIC CADENCE: Standard compliance evaluation cycle. Once every **24 hours**, assignments are automatically reevaluated. A large policy or initiative of many resources can take time, so there's no pre-defined expectation of when the evaluation cycle completes. Once it completes, updated compliance results are available in the portal and SDKs.
- ON-DEMAND EVALUATION SCAN: Instead of waiting 24 hours or triggering any of the other above events, the following Azure PowerShell is available:

```
Start-AzPolicyComplianceScan -ResourceGroupName 'MyRG'
```

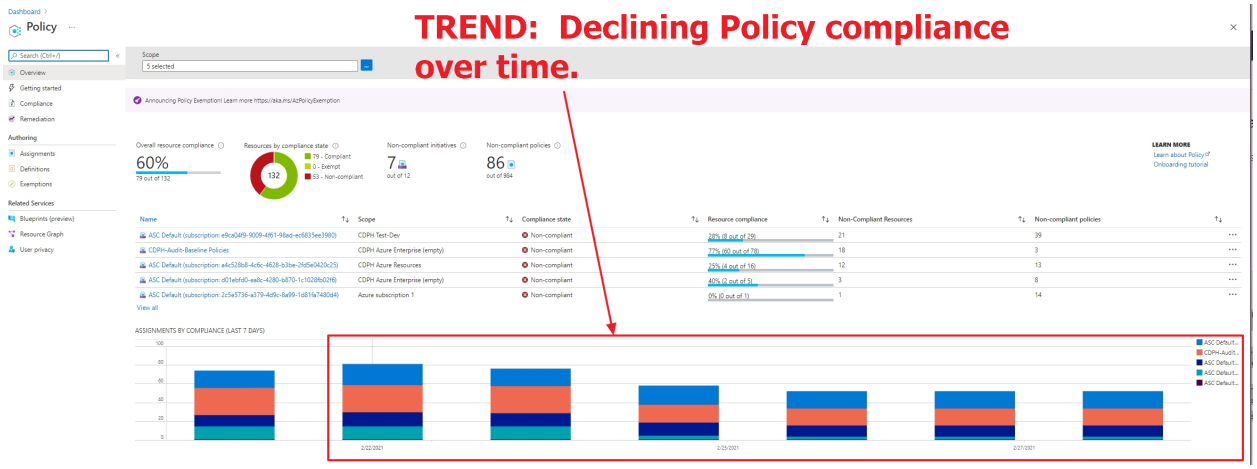
REFERENCE: Get policy compliance data - Azure Policy | Microsoft Docs

Determine causes of non-compliance

The Compliance Details pane (screen shot below left) displays information from the latest evaluation of the resource to the current policy assignment. Looking at the below right screen shot In this example, the location field's current value is "West US2" which does not match the resource group's location of "West US". This triggers a non-compliance assessment for the policy called "Audit resource location matches resource group location" policy.



The screen shot below of a CDPH lab environment highlights a trend of declining policy compliance over time. Trend analysis is yet another capability in the feature-rich Azure Policy section of the Azure Portal.



GOTCHA: If compliance state is being reported as "Not registered", verify that the Microsoft.PolicyInsights Resource Provider is registered and that the user has the appropriate Azure role-based access control (Azure RBAC) permissions as described in **Azure RBAC permissions in Azure Policy**.

Compliance Remediation

The effect settings you select for the policies you assign will determine your remediation options. You have two options available for remediation: manual and automatic.

- **Manual Remediation:** Manual remediation can be performed using the Azure portal or command-line options. This would depend on the policy objective and the complexity of remediation. As an example, updating the tag for the environment will be simpler than changing the virtual machine SKU. The manual remediation option will be more aligned with policies that are set to audit only. This is the first scenario for using Azure policy for existing environments that were set up before the compliance objects were agreed on or mandated for your organization.

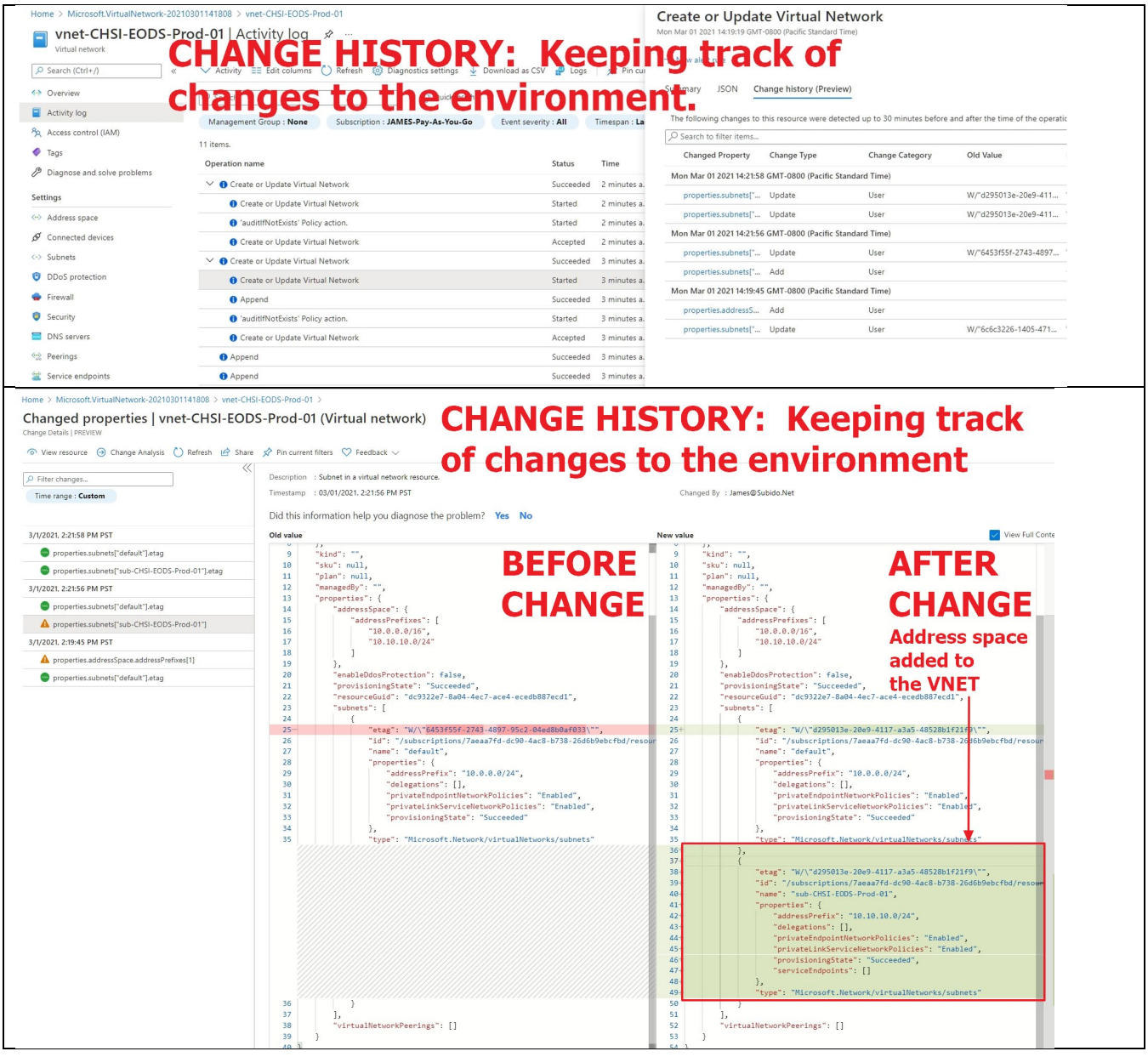
- **Automatic Remediation**: The second option is automatic remediation. This can be triggered through the policy service using the remediation node or your own automation tools and scripts that target the resources that are out of compliance. The option for remediation through the policy services is applicable to policies that use the *DeployIfNotExists* effect. You first assign a policy with the specified effect, and then create a remediation task to target non-compliant resources. The remediation task uses a security principal known as the managed identity, which is granted the security role appropriate to perform the remediation. The managed identity can be automatically created using the Azure policy definition or created manually.

At the time of this writing, the recommendation is for CDPH to perform remediation tasks manually. As its governance initiative evolves, CDPH may opt for the automatic remediation option.

Change History (Preview)

Tracking changes is critical and should be part of any governance process. CDPH's Azure cloud resources are changed through the course of daily use, reconfiguration, and redeployment. Change can come in the form of an administrator manually reconfiguring a resource or by an automated process.

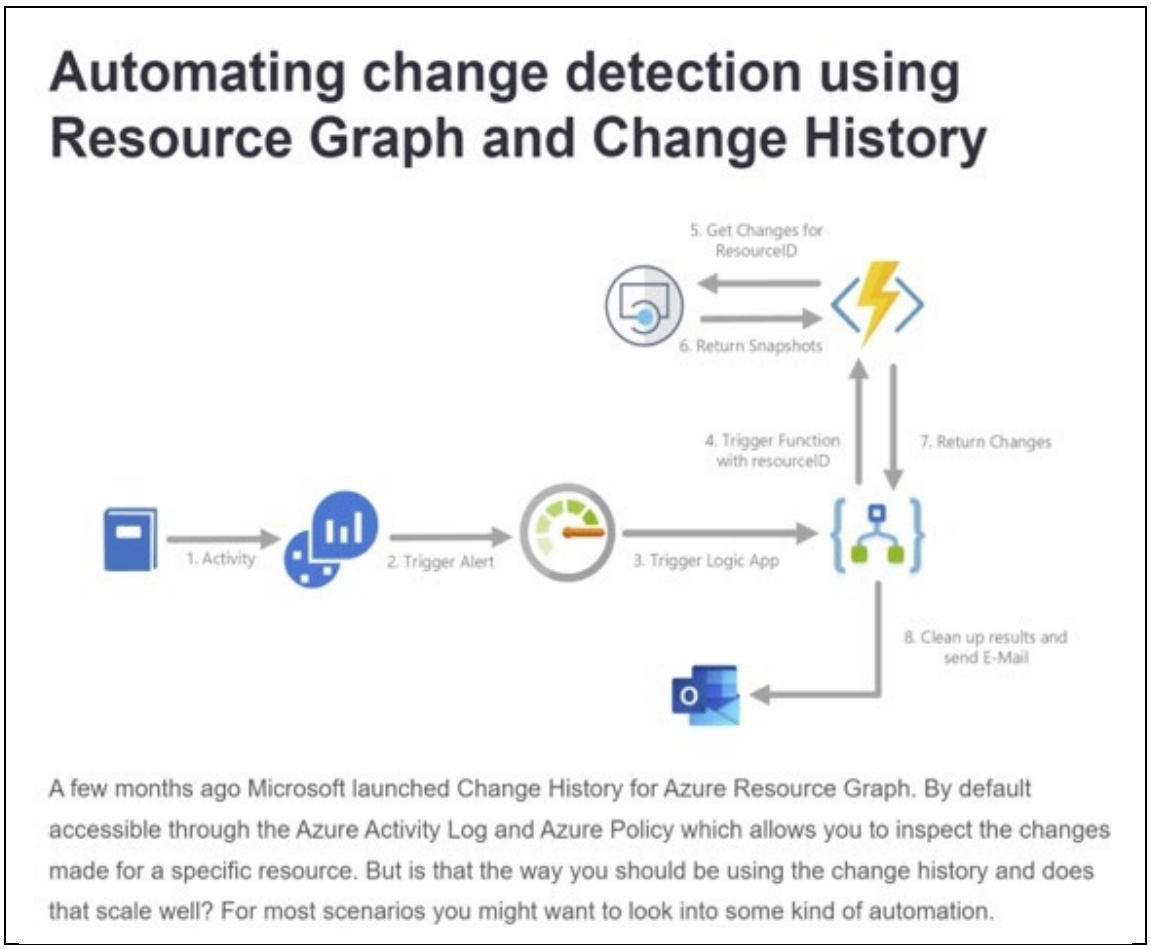
The following screen shot demonstrates the capability of Change History by capturing a change to an existing Virtual Network in the form of adding an address space:



As shown in the "After Change" column above, changes are always highlighted in green by Azure to easily identify them.

GOTCHA: Change History works only for Azure Resource Manager tracked properties. For example, changes inside a virtual machine or updates to data within a SQL Server are not tracked. For tracking changes inside a virtual machine see Azure Automation Change Tracking and Inventory overview | Microsoft Docs.

One consideration for automating change detection is using a series of Azure components such as Log Analytics, Azure Monitor Alerts, Logic App, and an Azure Function:



REFERENCE: Automating change detection using Resource Graph and Change History (wesleyhaakman.org)

Logging and Retention Strategy for Azure Platform Logs

Azure Platform Logs record the "Who? What? When? And Where?" of all user and service account activities in Azure. The default of 90 days for Activity Logs and 30 days for Azure Active Directory Sign-in and Audit logs is generally insufficient for acquiring historical information of these critical

activities for the purposes of security investigations, general troubleshooting, auditing access permissions, or facilitating da-to-day operations. Additionally, regulatory compliance requirements require a minimum of one year.

The table below lists the three types of platform logs:

Types of platform logs

The following table lists the specific platform logs that are available at different layers of Azure.

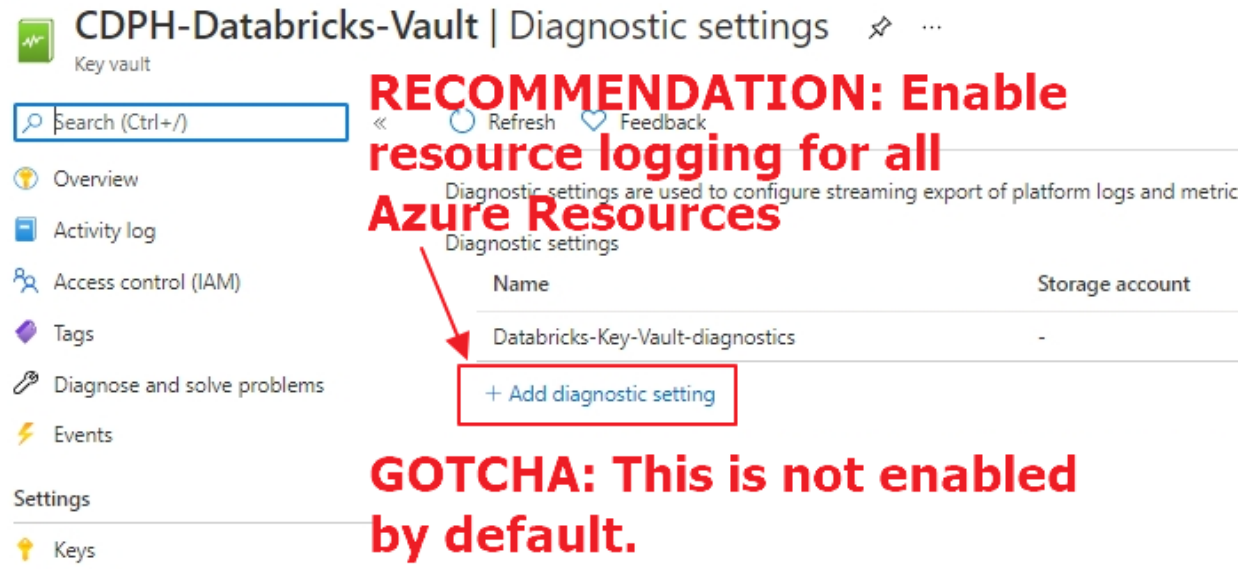
Log	Layer	Description
Resource logs	Azure Resources	Provide insight into operations that were performed within an Azure resource (the *data plane*), for example getting a secret from a Key Vault or making a request to a database. The content of resource logs varies by the Azure service and resource type. *Resource logs were previously referred to as diagnostic logs.*
Activity log	Azure Subscription	Provides insight into the operations on each Azure resource in the subscription from the outside (*the management plane*) in addition to updates on Service Health events. Use the Activity Log, to determine the *what, who,* and *when* for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. There is a single Activity log for each Azure subscription.
Azure Active Directory logs	Azure Tenant	Contains the history of sign-in activity and audit trail of changes made in the Azure Active Directory for a particular tenant.

SOURCE: Overview of Azure platform logs - Azure Monitor | Microsoft Docs

The default retention period for platform logs are as follows:

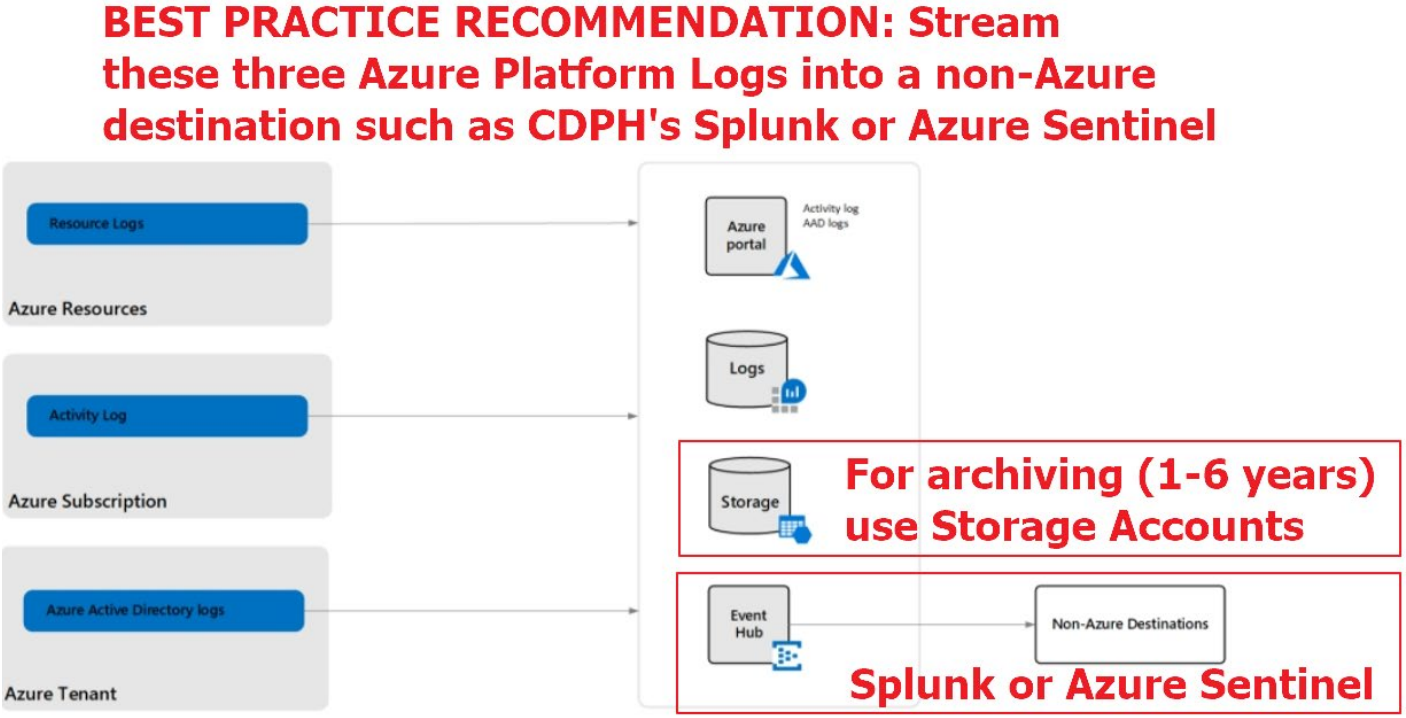
AZURE PLATFORM LOG NAME	DEFAULT RETENTION
Resource Logs *(formerly Diagnostic logs)*	Not applicable – not collected by default
Activity Logs	90 days
Azure Active Directory Logs	30 days for both sign-in and audit logs

GOTCHA: Resource Logs are not collected by default. You must create a diagnostic setting for each Azure resource to send its resource logs to an Event Hub (Splunk) or Azure Storage (long-term archiving). To send to both simultaneously, create a diagnostic setting for each.

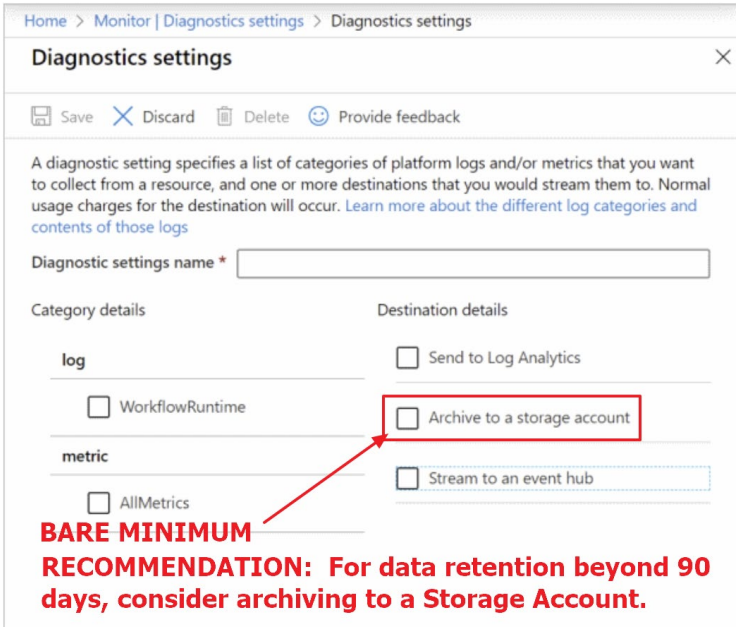


The recommended log retention for HIPAA compliance varies, with guidance recommending anywhere from one to six years. This governance framework will only provide guidance on a retention strategy (below). Please consult with CDPH's ISO for additional guidance on actual log retention requirements.

FOR DISCUSSION: Consult with CDPH's Information Security Officer (ISO) for guidance on establishing Azure platform logs' retention policies.

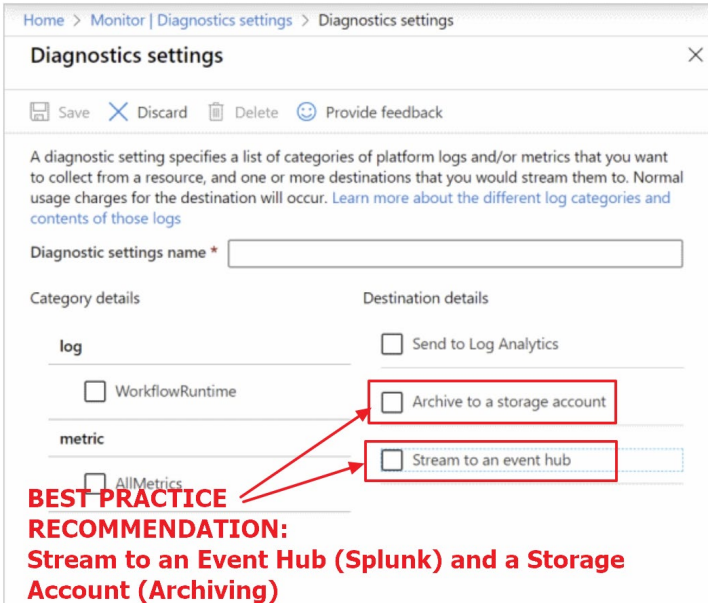


The bare minimum requirement will archive platform logs to an Azure storage account for long-term archiving. Compared with other mechanisms for archiving, Azure storage is less expensive, and data can be retained indefinitely. This bare minimum recommendation is actionable ASAP as it has no dependencies other than the requirement of a change control approval.



Utilizing a Security Information and Event Management (SIEM) solution such as Splunk or Azure Sentinel provides meaningful correlation between common attributes and events. It aggregates data from multiple sources in real time and generates actionable alerts based on anomalous conditions it detects and store data for a defined retention period.

The recommended approach is to stream platform logs into an Event hub then into Splunk for real-time alerting. For long-term archiving, platform logs can be archived into a storage account.



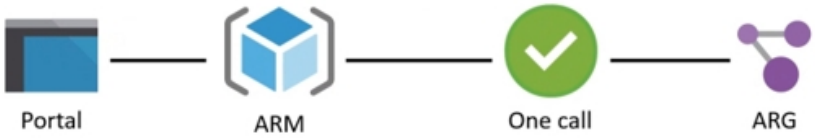
12. Azure Resource Graph

Resource Graph is an engine that will allow CDPH the ability to explore, query, and analyze its Azure resources at enterprise scale. Resource Graph is designed to extend Azure governance by providing efficient resource exploration across a given set of subscriptions.

You can think of Resource Graph as a large database containing all your Azure resources that can be queried using Kusto Query Language (KQL). These queries provide the following features:

Resource Graph key capabilities

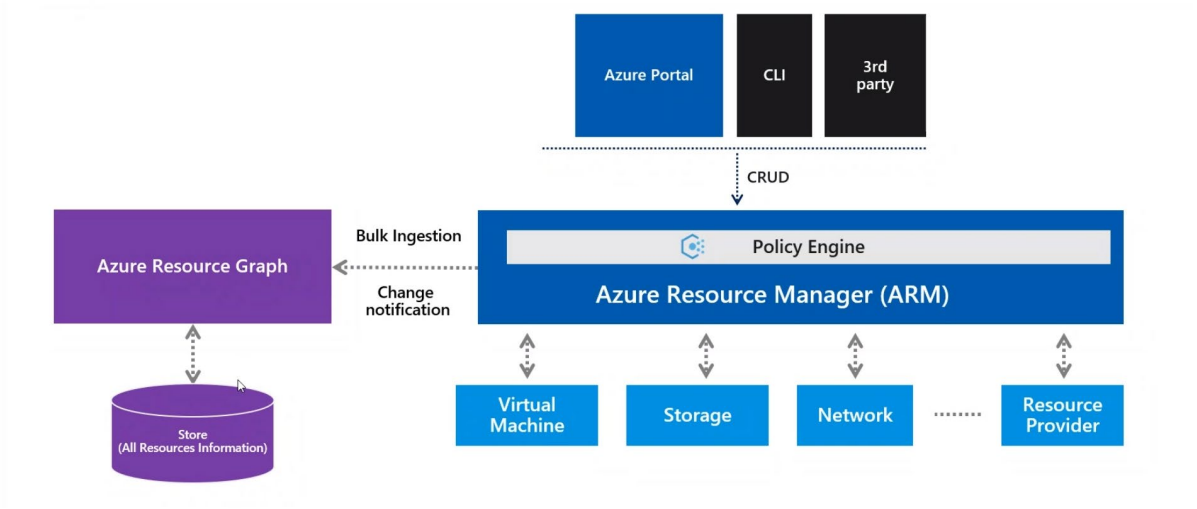
- Ability to query resources with complex filtering, grouping, and sorting by resource properties.
- Ability to iteratively explore resources based on governance requirements and convert the resulting expression into a policy definition.
- Ability to assess the impact of applying policies in a vast cloud environment.
- Ability to query Change History (discussed in *Chapter 15: Monitoring for Compliance and Changes*)
- Example: Azure Resource Graph is used by Azure portal's new browse 'All resources' experience. It is designed to help customers with a need to manage large-scale environments.



As soon as you create a new resource or update an existing resource, Azure Resource Manager (ARM) notifies Resource Graph of this change, and the Resource Graph database is updated accordingly. Additionally, in the event you update your resources outside of ARM, Resource Graph regularly runs a full scan of all resources, ensuring that the database is always current. The illustration below shows these elements as they relate to other Azure management plane components:

Azure Resource Graph

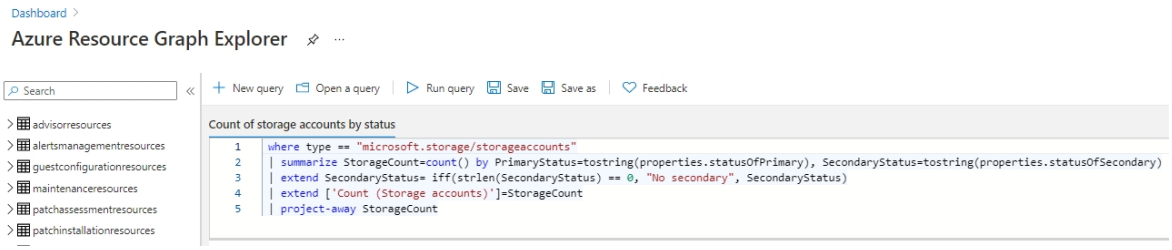
How it works



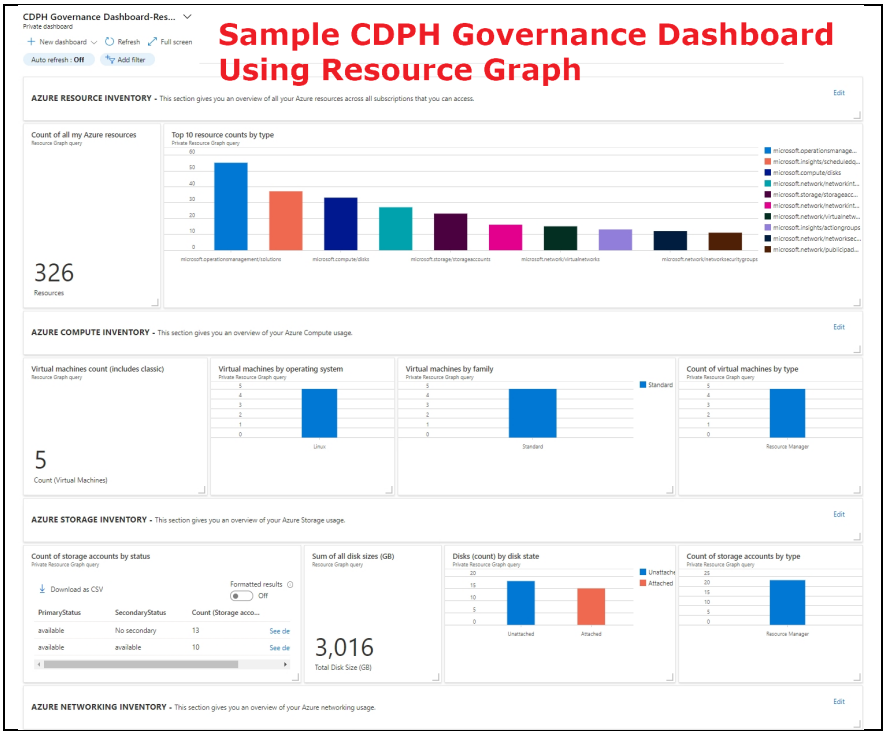
Here are a few queries that we can do on Resource Graph that will help CDPH with governance compliance:

- Query for resources without resource tags
- Query for resources with governance tags in place
- Query for unauthorized resources
- Query for storage accounts by status
- Query for changes using Change History (discussed in Chapter 15)
- Query for all Azure resources by type across all subscriptions

Here is an example of a Resource Graph query:



The results of these queries can be presented into a chart and displayed into a dashboard. Using custom dashboards, we can bring in all the above queries together into a single unified pane of glass that can be shared with other CDPH staff. Her is a screen shot of a sample CDPH Governance dashboard:



13. WHAT'S NEXT: How do we move forward from here?

PHASE 1: Decommission unused Azure Resources.

Almost four years old, CDPH's Azure environment contains unused resources. This phase will develop a process for decommissioning Azure resources which will cover the following areas:

1. Create a Cherwell Change Request
2. Develop a naming convention for resources about to be retired
3. Move resource to a retirement resource group
4. Remove all access to resource
5. Leave the resource inaccessible and renamed for a holding period of 30-60 days
6. After the holding period of 30-60 days has expired, permanently delete the resource

PHASE 2: Implement Resource Hierarchy and Naming Convention

Covered in chapter 6, the resource hierarchy will deploy a management group structure based on business units. As management groups are currently not in use, this will require moving resources around to their appropriate hierarchical tiers. A prerequisite is to assign each business unit and associated program with its own subscription.

Rolling out the naming convention for existing Azure resources will not be possible for most of CDPH's existing resources. A few resources can be renamed, such as subscriptions and resource groups (through the create a new resource group and move resources workaround). The rest of the resources will need to be left unchanged.

PHASE 3: Identify and Develop RBAC Roles for CDPH

Go through entire environment and identify necessary roles. Use built-in roles whenever possible and create custom roles only when necessary.

Map RBAC roles to Azure AD groups. Note that on-prem Active Directory groups are not supported for use in RBAC at this time. New Azure AD groups will need to be created.

PHASE 4: Lockdown and Protect the Resource Hierarchy

Resource groups (and the resources within), subscriptions, management groups and the tenant collectively constitute the resource hierarchy. Of crucial importance is the protection of the resource hierarchy from changes that could negatively impact CDPH's cloud datacenter.

With RBAC roles clearly defined and mapped to Azure AD groups from the previous phase, we can move forward with protecting CDPH's resource hierarchy by performing the following tasks:

- Clean-up existing RBAC that are based on individual user accounts
- Implement RBAC using AD groups
- Implement resource locks

PHASE 5: Implement Policies Through Two Initiatives

Key to CDPH's governance effort are policies. When many individual policies are group together, they comprise an initiative. Here is a list of the two initiatives currently for deployment. Note that the HITRUST/HIIPAA is a built-in initiative. With guidance from its ISO, CDPH Azure architecture team will need to go through each of the individual policies and determine which ones will be appropriate and suitable for deployment.

INITIATIVE #1: CDPH BASELINE INITIATIVE

1 Restrict all resources to WestUS region
2 Allowed resource types **O**R Deny resource types
3 Tagging (ACCOUNTABILITY-Owner) applied to resource groups.
4 Tagging (ACCOUNTABILITY-Creation Date) applied to resource groups.
5 Tagging (ACCOUNTABILITY-Business Unit) applied to resource groups.

6 Tagging (ACCOUNTABILITY-Cost Center) applied to resource groups.
7 Tagging (ACCOUNTABILITY-Cherwell Ticket) user prompted -- applied to resource groups.
8 Allowed Azure Region for Resources and Resource Groups
9 Allowed Storage Account SKUs (choose while deploying)
10 Allowed Azure VM SKUs (choose while deploying)
11 Require Network Watcher to be deployed
12 Require Azure Storage Account Secure Transfer Encryption
13 Deny resource types (choose while deploying)
14 Policy initiatives: Enable monitoring in Azure Security Center (100+ policy definitions)

INITIATIVE #2: CDPH HITRUST/HIPAA

NOTE: The 50 policies below come with the built-in HITRUST/HIPAA Initiative. A determination will need to be conducted on each policy as to whether it would be appropriate for CDPH's environment.

1 [Preview]: Container Registry should use a virtual network service endpoint
2 A maximum of 3 owners should be designated for your subscription
3 A vulnerability assessment solution should be enabled on your virtual machines
4 An activity log alert should exist for specific Administrative operations
5 Audit diagnostic setting
6 Audit usage of custom RBAC rules
7 Audit Windows machines missing any of specified members in the Administrators group
8 Audit Windows machines on which the Log Analytics agent is not connected as expected
9 Audit Windows machines that have extra accounts in the Administrators group
10 Azure Key Vault Managed HSM should have purge protection enabled
11 CORS should not allow every resource to access your Web Applications
12 Cosmos DB should use a virtual network service endpoint
13 Deprecated accounts with owner permissions should be removed from your subscription
14 Diagnostic logs in App Services should be enabled
15 Diagnostic logs in Azure Stream Analytics should be enabled
16 Diagnostic logs in Data Lake Analytics should be enabled
17 Diagnostic logs in Key Vault should be enabled
18 Diagnostic logs in Service Bus should be enabled
19 Enforce SSL connection should be enabled for MySQL database servers
20 Enforce SSL connection should be enabled for PostgreSQL database servers
21 Ensure WEB app has 'Client Certificates (Incoming client certificates)' set to 'On'
22 Event Hub should use a virtual network service endpoint
23 External accounts with owner permissions should be removed from your subscription
24 Function App should only be accessible over HTTPS
25 Geo-redundant backup should be enabled for Azure Database for MySQL
26 Geo-redundant backup should be enabled for Azure Database for PostgreSQL
27 Internet-facing virtual machines should be protected with network security groups
28 Key Vault should use a virtual network service endpoint
29 Latest TLS version should be used in your API App

30 Latest TLS version should be used in your Function App
31 Latest TLS version should be used in your Web App
32 Long-term geo-redundant backup should be enabled for Azure SQL Databases
33 MFA should be enabled on accounts with read permissions on your subscription
34 Microsoft Antimalware for Azure should be configured to automatically update protection signatures
35 Monitor missing Endpoint Protection in Azure Security Center
36 Network Watcher should be enabled
37 Resource logs in Azure Key Vault Managed HSM should be enabled
38 SQL Server should use a virtual network service endpoint
39 Storage Accounts should use a virtual network service endpoint
40 Subnets should be associated with a Network Security Group
41 The Log Analytics agent should be installed on Virtual Machine Scale Sets
42 The Log Analytics agent should be installed on virtual machines
43 Virtual machines should be connected to an approved virtual network
44 Vulnerabilities in container security configurations should be remediated
45 Vulnerabilities in security configuration on your machines should be remediated
46 Vulnerabilities on your SQL databases should be remediated
47 Vulnerability assessment should be enabled on your SQL servers
48 Web Application should only be accessible over HTTPS
49 Windows machines should meet requirements for 'Security Options - User Account Control'
50 Windows machines should meet requirements for 'User Rights Assignment'

PHASE 6: Develop a Process for Governance

This phase will seek to develop a process that ensures that governance is not a one-time effort and that it persists beyond this document.

PHASE 7: Implement Cost Management

This allocation of unique Azure subscriptions to business unit managers is the key to establishing their role in cost management accountability. A unique subscription would empower them to establish budgets, develop alerting measures through email and SMS text, generate reports, receive optimization advice, and proactively address forecasted costs based on existing estblished utilization patterns.

This phase will provide access to the Azure Portal for each business unit manager. Their access will be restricted only for performing cost management functions.

PHASE 8: Implement Blueprints

A Blueprint is a repeatable template that CDPH's architecture team defines once and then deploys during the creation of new management groups and subscriptions. This allows CDPH to define its

governance through RBAC and policies then encapsulate them into a Blueprint for rapid deployment to stand up new fully governed environments.

------- End of Document ---------