Partner Earned Credit

Contents

1. What is Partner Earned Credit (PEC)?

Partner earned credit (PEC) is a partner reward mechanism for Azure in Microsoft's new commerce experience in Cloud Solution Provider (CSP). It is designed to support a partner ecosystem focused on value-added managed services as well as help customer and partners with unified Azure pricing across all of Microsoft Go-To-Market vehicles. By focusing on specific partner business activities, PEC will help mitigate price-based competition and better support a value-added services ecosystem.

With thousands of services in Azure and multiple options to buy, pricing can be challenging for many customers and partners. In the new commerce experience for Azure, we have aligned to single global pricing principles applicable to all motions we transact. CSP partners can provide greater transparency to their customers and build trust by offering Azure at published prices.

The digital transformation of our customers requires an expanded set of activities and value from Azure partners. Many customers look for partners to provide services above and beyond pure billing/transaction to help their cloud journey and allow to consume Azure services efficiently. Microsoft partners play a critical role in all stages of the customer lifecycle by helping the customer navigate the complex Azure journey and enable consumption. These kind of partner services are **on-going in nature** and include Azure estate monitoring, policy and governance management, set up and configuration fine-tuning, technical support and a variety of other services. All these services require a partner to be intimately familiar with the customer's Azure environment and having **continuous and appropriate governance and control** to the underlying resources they provide management on. Partners providing this **24 X 7 cloud operations management activity** will become eligible for a "Partner earned credit for services managed" on the customers' Azure estate governed and controlled by the partner.

2. The benefits to Customers and Partners

- Customers can outsource their Azure Infrastructure management and billing to trustworthy and qualified partners and focus on their core business activities.
- Customers who need assistance in consuming Azure get to work with partners invested in managed services on Azure that can drive cost and operational efficiencies.
- Partners are rewarded because they provide a robust managed services portfolio on Azure for their customers.
- Intimate association and management of Customer's Azure projects will bring new opportunities to partner and help drive consumption growth.

3. Considerations for Partners

As customers transition to cloud computing platforms, they are faced with managing not just a new set of technologies, but also a new way of approaching management and operations of their digital estate. While the cloud can bring greater business value and agility, it can also bring new concerns, including lack of proper security and cost control.

Azure Partners have an opportunity to help customers understand how to manage, automate, and optimize their digital estate hosted on Microsoft Azure. With managed services, Azure partners can help customers on a continuous basis through day-to-day operations and support services which include:

- **Cloud Operations & Management Services:** Customers look to Microsoft partners to reduce costs in Azure while reproducing the isolation, security policies, and audit models they have today. They also expect partners to have mature practice and processes for identifying workload suitability and ongoing operational costs of Azure. Automation and orchestration, patching updates, configuration management, backup and disaster recovery, and identity management are tasks that customers expect partners to operate and manage.

- **Cloud Monitoring & Technical Support**: In a cloud consumption world, the tools and requirements have evolved, but the concern of finding the right resource for managing IT infrastructure hasn't changed. Most organizations simply do not have the time, resources, or dedicated staff required to monitor every aspect of IT, and this is where Managed Services Partners (MSPs) add the most value. While Azure offers many monitoring capabilities built within the platform, partners who (a) provide additional, deeper monitoring tooling (b) triage the false positives from the real alerts, and, (c) proactively act upon the alerts before any measurable loss in performance; play an important role on ongoing managing of their customers' Azure estate:
    - **SYSTEM HEALTH MONITORING:** Complete monitoring of VMs, CPU utilization, memory usage, storage IOPs, and OS performance. Includes monitoring of application performance and operation health, and dashboards and reports on system health.
    - **LOG ANALYTICS AND ALERTING:** Every client, device, and user accessing a network produces data that is logged. Analyzing those logs can offer deep insight into performance, security, resource consumption, and several other meaningful metrics.
    - **DATABASE MONITORING:** A view into customer's database that helps MSPs ensure high availability of database servers. The process involves keeping logs of size, connection time and users of databases, analyzing use trends, and leveraging data to proactively remediate issues
    - **APP PERFORMANCE MONITORING:** End-to-end tracking of all aspects of an application (or webpage). App monitoring involves watching every part — from shopping carts to registration pages — of a customer's app(s) for performance issues to provide the best user experience possible.

Click here to learn more about how to expand your managed services portfolio with Azure

All these services entail an appropriate access for partners into customer's Azure environment and our commerce system will measure this access details to calculate the PEC

Customers have the option to remove any access given to their partners. Partners should not coerce customers to assign them appropriate access for the sole purpose of earning PEC from Microsoft - failure to adhere with the above requirement might make the partner ineligible to earn PEC.

4. How is Partner Earned Credit (PEC) calculated and paid?

PEC recognizes and rewards partners that own the 24x7 IT operational control and management of parts or the entire Azure environment of their customers in CSP. By default, in CSP, partners are granted the necessary access rights to the customer's subscription that allow them to perform 24x7 operational management and control of the resources on the subscription. Additional ways in which customer can provision access for transacting partner is described in section 5. The monthly invoice amount is net of PEC and partner can see the details on their monthly recon file.

Important eligibility and calculation information

- Partner should have an active MPN agreement and valid RBAC role to get earned credit for the azure assets they manage (Refer to appendix (A) for valid roles)
- In the case of Indirect providers and their indirect resellers, the indirect provider will be eligible for PEC if either the indirect provider, or the indirect reseller or both (indirect provider and indirect reseller) have 24x7 operational control and management of the customer's Azure resources in CSP.
- PEC is associated to billed (Chargeable) consumption of customer's Azure estate in CSP managed by the partner. PEC is made available only to partners in CSP billed by Microsoft (Indirect Provider, Direct Bill Partner).
- Eligible Services: PEC is applicable to Azure services given on the price list (Click on "Export Azure plan price list"). Please note there are exceptions including, but not limited to, third-party, Azure Reservations and Marketplace items.
- PEC is calculated daily and can be viewed in the daily recon file and monthly invoice recon file. A Partner (provider or reseller in the case of Tier 2) must have access for the entire day (24x7) to ensure they earn PEC.
- PEC details are shown in the invoice recon file.
- PEC is earned down at the Azure resource level. If the partner has valid access at the subscription, or resource group level each resource that role up to the higher entity will earn PEC.
- Partners can view PEC details for their customers' Azure consumption on Azure Cost management. Learn more

5. Partner's Access to manage Azure Subscriptions

Partners can earn PEC by providing value added services which require 24x7 operational control and management of customer's Azure resources. In CSP there are different options available for provisioning the required access to perform value added services. The various role-based access control (RBAC) methods are

- Partners with a direct billing relationship with Microsoft, that provision a new subscription for a customer are granted 24x7 operational control and management by default. **Admin on Behalf Of (AOBO)** – With AOBO, any user with the Admin Agent role in partner tenant will have RBAC owner access to Azure subscriptions that you create through the CSP program. The customer can manage access by navigating to the Access Control section on the Azure Portal. Within the Role Assignments tab, they can choose to change the partner's AOBO Access. If this is desired by the customer explore the following options with the customer.

- **Azure Lighthouse**: AOBO doesn't provide the flexibility to create distinct groups that work with different customers, or to enable different roles for groups or users. Using Azure Lighthouse, you can assign different groups to different customers or roles. Because users will have the appropriate level of access through Azure delegated resource management, you can reduce the number of users who have the Admin Agent role (and thus have full AOBO access). This helps improve security by limiting unnecessary access to your customers' resources. It also gives you more flexibility to manage multiple customers at scale. For more information, please refer to Azure Lighthouse and the Cloud Solution Provider program.

- **Directory or Guest Users or Service Principals:** Customer can delegate granular access to Azure resources in CSP subscriptions by adding users in the customer directory or adding guest users and assign any RBAC roles. More details can be found here

Microsoft recommends partners to leverage RBAC roles diligently using the best security practices with least access principle (users have bare minimum permissions they need to perform their work).

How to Link Partner ID (MPN ID) for various RBAC Options

To reward partners for services they provide to customers, the existing margin in Azure in CSP is evolving to the partner earned credit for services managed (PEC). To receive PEC, you need to link the partner ID with the credentials used for managing Customer's Azure resources. Following tables show methods to associate the partner ID with various RBAC access options –

Category	**Scenario**	**MPN ID Association**
AOBO	CSP Direct Bill partner or Indirect Provider creates the subscription for the customer, CSP Direct or Indirect Provider is default owner of the subscription using AOBO	Automatic (No Partner work required)
	CSP Direct Bill partner or Indirect Provider gives access of the subscription to Indirect Reseller using AOBO.	
Azure Lighthouse	Partner creates a new Managed Services offer in Marketplace, this offer is accepted on the CSP subscription and partner gets access to the CSP subscription	Automatic (No Partner work required)
	Partner deploys ARM template in Azure subscription	Partner needs to associate MPN ID to the user or service principal in the partner tenant More Information – Link Partner ID
Directory or Guest User	Partner creates a new user or service principal in the customer directory and give access of the CSP subscription to the user.	Partner needs to associate MPN ID to the user or service principal in the customer tenant. More Information – Link Partner ID
	Partner creates a new user or service principal in the customer directory, add the user to group and give access of the CSP Subscription to the group.	

6. Security and Access control practices

Partner Security Requirements

Greater privacy safeguards and security are among our top priorities. We know that the best defense is prevention and that we are only as strong as our weakest link. That is why we need everyone in our ecosystem to act and ensure they have appropriate security protections in place. To help safeguard partners and customers, we're introducing a set of mandatory security requirements for Advisors, Control Panel Vendors, and partners participating in the Cloud Solution Provider program.

Partners who do not implement the mandatory security requirements will not be able to transact in the CSP program or manage customer tenants leveraging delegate admin rights, once these requirements are enforced. We are in the process of establishing a technical enforcement date for the requirements and will notify partners of the date with detailed information.

What actions do partners need to take?

Given the highly privileged nature of being a partner we need to ensure that each user has an MFA challenge for every single authentication. This can be accomplished through one of the following ways

- Implementing Azure AD Premium and ensure that MFA is enforced for each user
- Implementing the baseline protection policies
- Implementing a third-party solution and ensure MFA is enforced for each user

Starting August 1, 2019, all partners are required to enforce multi-factor authentication in their partner tenant. Detailed information on these security requirements can be found at https://docs.microsoft.com/partner-center/partner-security-requirements.

Partners can gain 24x7 operational control and management of a customer's Azure resources in CSP by leveraging different options provided through the role-based access control feature (RBAC). Microsoft recommends partners to leverage RBAC diligently, following best practices enabled through Azure Active Directory Privileged Identity Management resources.

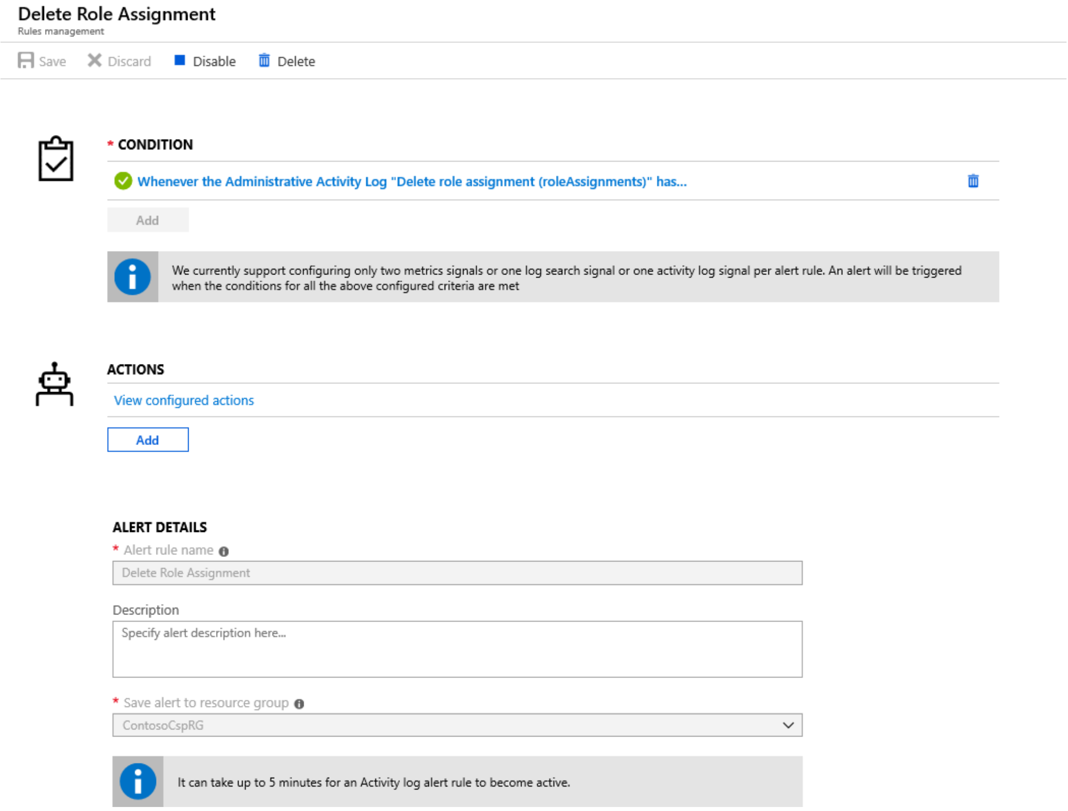
7. How to validate whether the partner is earning PEC for usage?

There are several ways a partner can confirm they are earning PEC on customer's Azure resources managed:

- Review the daily usage file **here**. The unit price and effective unit price within the daily usage file will be different if PEC has been applied. (Note there are other pricing factors that could cause the unit price and effective price to be different other than when PEC is earned)
- View PEC details for customers' Azure consumption on Azure Cost management experience. Learn more
- Additionally, create an Azure Monitor Alert for notifications on change of roles

You can create an Azure Monitor activity log alerts to receive the notification when your RBAC access is removed from CSP subscription.

1) Create Alert



Delete Role Assignment

Rules management

* CONDITION

Whenever the Administrative Activity Log "Delete role assignment (roleAssignments)" has...

We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met

ACTIONS

ALERT DETAILS

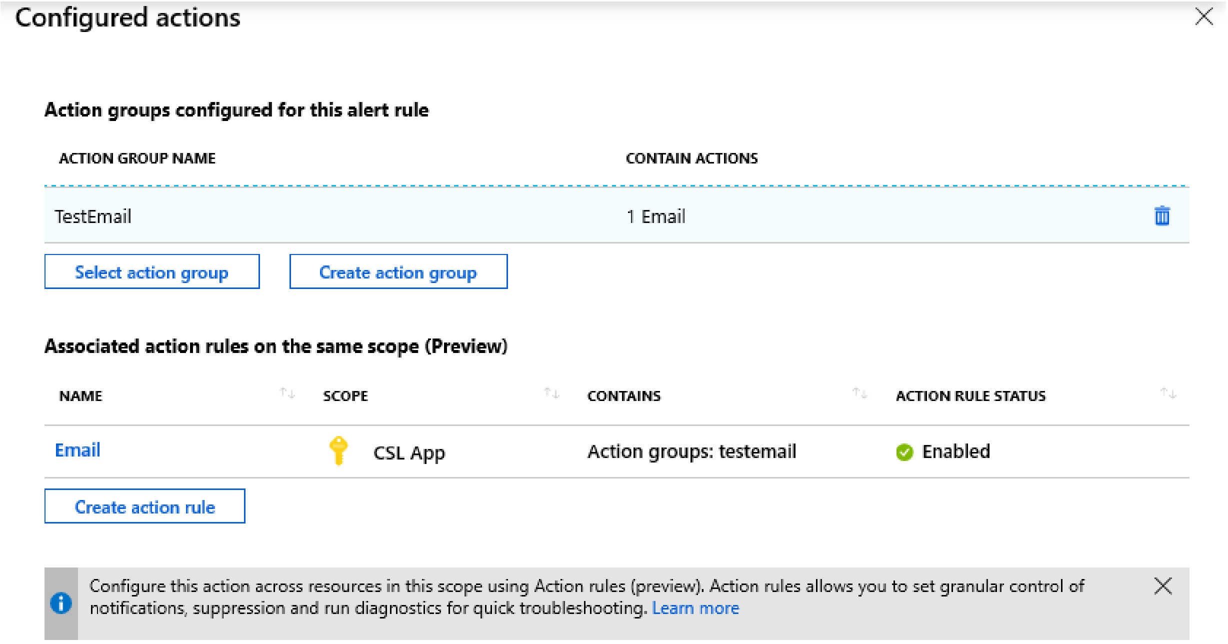
* Alert rule name: Delete Role Assignment

Description: Specify alert description here...

* Save alert to resource group: ContosoCspRG

It can take up to 5 minutes for an Activity log alert rule to become active.

2) Configure the action that you will like to take on the alert (Example – Email, Webhook etc.)



Configured actions

Action groups configured for this alert rule

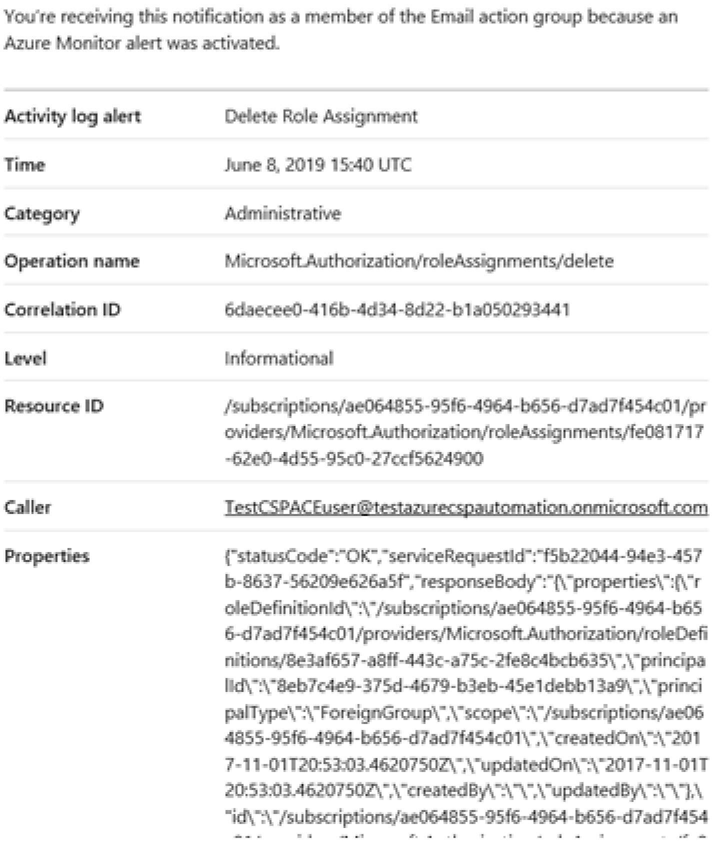
ACTION GROUP NAME	CONTAIN ACTIONS
TestEmail	1 Email

Associated action rules on the same scope (Preview)

NAME	SCOPE	CONTAINS	ACTION RULE STATUS
Email	CSL App	Action groups: testemail	✓ Enabled

Configure this action across resources in this scope using Action rules (preview). Action rules allows you to set granular control of notifications, suppression and run diagnostics for quick troubleshooting. Learn more

If you have specified the action as an email, you will receive an email notification if any role assignment deletion occurs.



You're receiving this notification as a member of the Email action group because an Azure Monitor alert was activated.

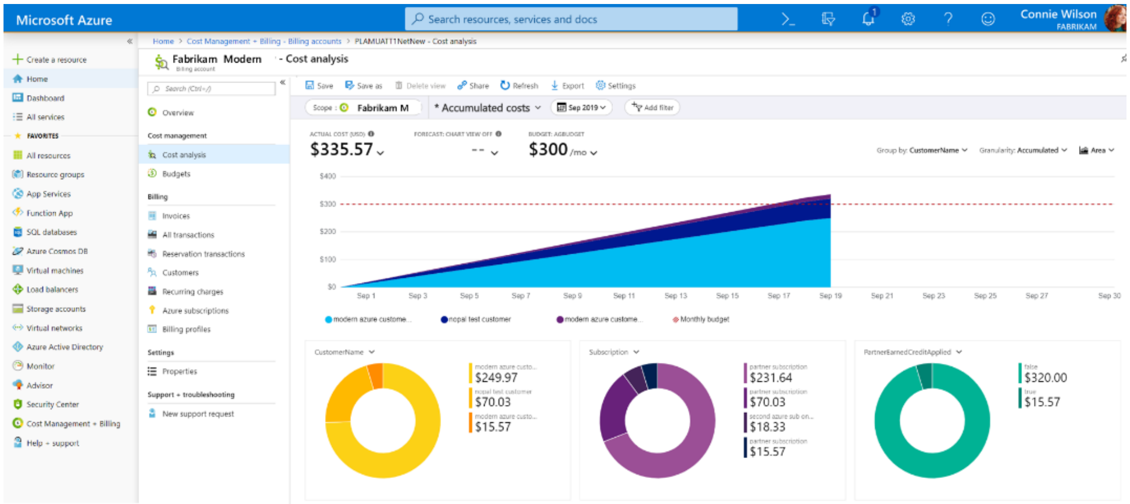
Activity log alert	Delete Role Assignment
Time	June 8, 2019 15:40 UTC
Category	Administrative
Operation name	Microsoft.Authorization/roleAssignments/delete
Correlation ID	6daecee0-416b-4d34-8d22-b1a050293441
Level	Informational
Resource ID	/subscriptions/ae064855-95f6-4964-b656-d7ad7f454c01/providers/Microsoft.Authorization/roleAssignments/fe081717-62e0-4d55-95c0-27ccf5624900
Caller	TestCSPACEuser@testazurecspautomation.onmicrosoft.com
Properties	{"statusCode":"OK","serviceRequestId":"f5b22044-94e3-457b-8637-56209e626a5f","responseBody":"{\"properties\":{\"roleDefinitionId\":\"/subscriptions/ae064855-95f6-4964-b656-d7ad7f454c01/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635\",\"principalId\":\"8eb7c4e9-375d-4679-b3eb-45e1debb13a9\",\"principalType\":\"ForeignGroup\",\"scope\":\"/subscriptions/ae064855-95f6-4964-b656-d7ad7f454c01\",\"createdOn\":\"2017-11-01T20:53:03.4620750Z\",\"updatedOn\":\"2017-11-01T20:53:03.4620750Z\",\"createdBy\":\"\",\"updatedBy\":\"\"},\"id\":\"/subscriptions/ae064855-95f6-4964-b656-d7ad7f454

8. Azure Cost Management

View the charges for resources that have PEC applied in Azure Cost Management (ACM)

In ACM, Cost Analysis enables you as a partner to view the costs that have received the benefit of PEC.

1. In the Azure Portal, login into the partner tenant and click on **Cost Management + Billing**
2. Click on **Cost Management**
3. Click on **Cost Analysis**
   The Cost Analysis view will display the costs for the partner billing account, for all the services purchased and consumed at the prices that the partner pays Microsoft .
4. Select **PartnerEarnedCreditApplied** in the drop down on a pivot chart to slice and dice costs that have PEC applied. When **PartnerEarnedCreditApplied** property is ***True***, the associated cost has the benefit of the partner earned admin access.
   When the **PartnerEarnedCreditApplied** property is ***False***, the associated cost has not met the required eligibility for the credit or the service purchased is not eligible for partner earned credit
   Note:. Typically, **<u>usage for services takes 8-24 hours</u>** to appear in Cost Management and the PEC credits will appear within 48 hours from time of access in Azure Cost Management.



Scope : Fabrikam M

* Accumulated costs

Sep 2019

ACTUAL COST (USD) $335.57

FORECAST: CHART VIEW OFF --

BUDGET: AGBUDGET $300 /mo

Group by: CustomerName

Granularity: Accumulated

Area

CustomerName

modern azure custo...	$249.97
nopal test customer	$70.03
modern azure custo...	$15.57

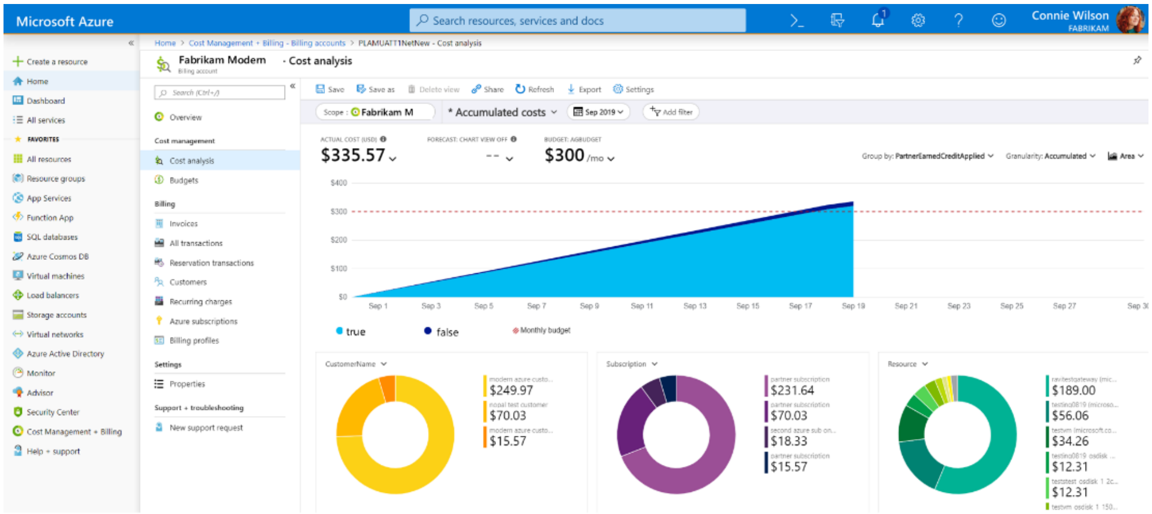
Subscription

partner subscription	$231.64
partner subscription	$70.03
second azure sub on...	$18.33
partner subscription	$15.57

PartnerEarnedCreditApplied

false	$320.00
true	$15.57

5. You can also group by and filter by the **PartnerEarnedCreditApplied** property using the **Group by** and **Add Filter** features to slice, dice and drill into costs that have PEC and the costs that have no PEC applied.



9. Additional resources

a. Appendix A

Partner Admin Link role mapping to permission level. Reader level permission does not qualify for earned credit.

Built-in role	Description	PEC Eligible
Owner	Lets you manage everything, including access to resources.	Yes
Contributor	Lets you manage everything except granting access to resources.	Yes
Reader	Lets you view everything, but not make any changes.	No
AcrDelete	acr delete	Yes
AcrImageSigner	acr image signer	Yes
AcrPull	acr pull	Yes
AcrPush	acr push	Yes
AcrQuarantineReader	acr quarantine data reader	No
AcrQuarantineWriter	acr quarantine data writer	Yes

API Management Service Contributor	Can manage service and the APIs	Yes
API Management Service Operator Role	Can manage service but not the APIs	Yes
API Management Service Reader Role	Read-only access to service and APIs	No
Application Insights Component Contributor	Can manage Application Insights components	Yes
Application Insights Snapshot Debugger	Gives user permission to view and download debug snapshots collected with the Application Insights Snapshot Debugger. Note that these permissions are not included in the Owner or Contributor roles.	Yes
Automation Job Operator	Create and Manage Jobs using Automation Runbooks.	Yes
Automation Operator	Automation Operators are able to start, stop, suspend, and resume jobs	Yes
Automation Runbook Operator	Read Runbook properties - to be able to create Jobs of the runbook.	Yes
Avere Contributor	Can create and manage an Avere vFXT cluster.	Yes
Avere Operator	Used by the Avere vFXT cluster to manage the cluster	Yes
Azure Event Hubs Data Owner	Allows for full access to Azure Event Hubs resources.	Yes

Azure Event Hubs Data Receiver	Allows receive access to Azure Event Hubs resources.	Yes
Azure Event Hubs Data Sender	Allows send access to Azure Event Hubs resources.	Yes
Azure Kubernetes Service Cluster Admin Role	List cluster admin credential action.	Yes
Azure Kubernetes Service Cluster User Role	List cluster user credential action.	Yes
Azure Maps Data Reader (Preview)	Grants access to read map related data from an Azure maps account.	No
Azure Service Bus Data Owner	Allows for full access to Azure Service Bus resources.	Yes
Azure Service Bus Data Receiver	Allows for receive access to Azure Service Bus resources.	Yes
Azure Service Bus Data Sender	Allows for send access to Azure Service Bus resources.	Yes
Azure Stack Registration Owner	Lets you manage Azure Stack registrations.	Yes
Backup Contributor	Lets you manage backup service, but can't create vaults and give access to others	Yes
Backup Operator	Lets you manage backup services, except removal of backup, vault creation and giving access to others	Yes
Backup Reader	Can view backup services, but can't make changes	No
Billing Reader	Allows read access to billing data	No

BizTalk Contributor	Lets you manage BizTalk services, but not access to them.	Yes
Blockchain Member Node Access (Preview)	Allows for access to Blockchain Member nodes	Yes
Blueprint Contributor	Can manage blueprint definitions, but not assign them.	Yes
Blueprint Operator	Can assign existing published blueprints, but cannot create new blueprints. NOTE: this only works if the assignment is done with a user-assigned managed identity.	Yes
CDN Endpoint Contributor	Can manage CDN endpoints, but can’t grant access to other users.	Yes
CDN Endpoint Reader	Can view CDN endpoints, but can’t make changes.	No
CDN Profile Contributor	Can manage CDN profiles and their endpoints, but can’t grant access to other users.	Yes
CDN Profile Reader	Can view CDN profiles and their endpoints, but can’t make changes.	No
Classic Network Contributor	Lets you manage classic networks, but not access to them.	Yes
Classic Storage Account Contributor	Lets you manage classic storage accounts, but not access to them.	Yes
Classic Storage Account Key Operator Service Role	Classic Storage Account Key Operators are allowed to list and regenerate keys on Classic Storage Accounts	Yes

Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	Yes
Cognitive Services Contributor	Lets you create, read, update, delete and manage keys of Cognitive Services.	Yes
Cognitive Services Data Reader (Preview)	Lets you read Cognitive Services data.	No
Cognitive Services User	Lets you read and list keys of Cognitive Services.	No
Cosmos DB Account Reader Role	Can read Azure Cosmos DB account data. See DocumentDB Account Contributor for managing Azure Cosmos DB accounts.	No
Cosmos DB Operator	Lets you manage Azure Cosmos DB accounts, but not access data in them. Prevents access to account keys and connection strings.	Yes
CosmosBackupOperator	Can submit restore request for a Cosmos DB database or a container for an account	Yes
Cost Management Contributor	Can view costs and manage cost configuration (e.g. budgets, exports)	Yes
Cost Management Reader	Can view cost data and configuration (e.g. budgets, exports)	No
Data Box Contributor	Lets you manage everything under Data Box Service except giving access to others.	Yes

Data Box Reader	Lets you manage Data Box Service except creating order or editing order details and giving access to others.	No
Data Factory Contributor	Create and manage data factories, as well as child resources within them.	Yes
Data Lake Analytics Developer	Lets you submit, monitor, and manage your own jobs but not create or delete Data Lake Analytics accounts.	Yes
Data Purger	Can purge analytics data	Yes
DevTest Labs User	Lets you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.	Yes
DNS Zone Contributor	Lets you manage DNS zones and record sets in Azure DNS, but does not let you control who has access to them.	Yes
DocumentDB Account Contributor	Can manage Azure Cosmos DB accounts. Azure Cosmos DB is formerly known as DocumentDB.	Yes
EventGrid EventSubscription Contributor	Lets you manage EventGrid event subscription operations.	Yes
EventGrid EventSubscription Reader	Lets you read EventGrid event subscriptions.	No
HDInsight Cluster Operator	Lets you read and modify HDInsight cluster configurations.	Yes
HDInsight Domain Services Contributor	Can Read, Create, Modify and Delete Domain Services related operations	Yes

	needed for HDInsight Enterprise Security Package	
Intelligent Systems Account Contributor	Lets you manage Intelligent Systems accounts, but not access to them.	Yes
Key Vault Contributor	Lets you manage key vaults, but not access to them.	Yes
Lab Creator	Lets you create, manage, delete your managed labs under your Azure Lab Accounts.	Yes
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; creating and configuring Automation accounts; adding solutions; and configuring Azure diagnostics on all Azure resources.	Yes
Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure diagnostics on all Azure resources.	No
Logic App Contributor	Lets you manage logic apps, but not change access to them.	
Logic App Operator	Lets you read, enable, and disable logic apps, but not edit or update them.	Yes

Managed Application Operator Role	Lets you read and perform actions on Managed Application resources	Yes
Managed Applications Reader	Lets you read resources in a managed app and request JIT access.	No
Managed Identity Contributor	Create, Read, Update, and Delete User Assigned Identity	Yes
Managed Identity Operator	Read and Assign User Assigned Identity	Yes
Management Group Contributor	Management Group Contributor Role	Yes
Management Group Reader	Management Group Reader Role	No
Monitoring Contributor	Can read all monitoring data and edit monitoring settings. See also Get started with roles, permissions, and security with Azure Monitor.	Yes
Monitoring Metrics Publisher	Enables publishing metrics against Azure resources	Yes
Monitoring Reader	Can read all monitoring data (metrics, logs, etc.). See also Get started with roles, permissions, and security with Azure Monitor.	No
Network Contributor	Lets you manage networks, but not access to them.	Yes
New Relic APM Account Contributor	Lets you manage New Relic Application Performance Management accounts and applications, but not access to them.	Yes
Reader and Data Access	Lets you view everything but will not let you delete or create a storage account or	Yes

	contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.	
Redis Cache Contributor	Lets you manage Redis caches, but not access to them.	Yes
Resource Policy Contributor (Preview)	(Preview) Backfilled users from EA, with rights to create/modify resource policy, create support ticket and read resources/hierarchy.	Yes
Scheduler Job Collections Contributor	Lets you manage Scheduler job collections, but not access to them.	Yes
Search Service Contributor	Lets you manage Search services, but not access to them.	Yes
Security Admin	In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations	Yes
Security Manager (Legacy)	This is a legacy role. Please use Security Administrator instead	Yes
Security Reader	In Security Center only: Can view recommendations and alerts, view security policies, view security states, but cannot make changes	No
Site Recovery Contributor	Lets you manage Site Recovery service except vault creation and role assignment	Yes

Site Recovery Operator	Lets you failover and failback but not perform other Site Recovery management operations	Yes
Site Recovery Reader	Lets you view Site Recovery status but not perform other management operations	No
Spatial Anchors Account Contributor	Lets you manage spatial anchors in your account, but not delete them	Yes
Spatial Anchors Account Owner	Lets you manage spatial anchors in your account, including deleting them	Yes
Spatial Anchors Account Reader	Lets you locate and read properties of spatial anchors in your account	No
SQL DB Contributor	Lets you manage SQL databases, but not access to them. Also, you can't manage their security-related policies or their parent SQL servers.	Yes
SQL Managed Instance Contributor	Lets you manage SQL Managed Instances and required network configuration, but can’t give access to others.	Yes
SQL Security Manager	Lets you manage the security-related policies of SQL servers and databases, but not access to them.	Yes
SQL Server Contributor	Lets you manage SQL servers and databases, but not access to them, and not their security -related policies.	Yes
Storage Account Contributor	Permits management of storage accounts. Provides access to the account key, which	Yes

	can be used to access data via Shared Key authorization.	
Storage Account Key Operator Service Role	Permits listing and regenerating storage account access keys.	Yes
Storage Blob Data Contributor	Read, write, and delete Azure Storage containers and blobs. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	Yes
Storage Blob Data Owner	Provides full access to Azure Storage blob containers and data, including assigning POSIX access control. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	Yes
Storage Blob Data Reader	Read and list Azure Storage containers and blobs. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	No
Storage Blob Delegator	Get a user delegation key, which can then be used to create a shared access signature for a container or blob that is signed with Azure AD credentials. For more information, see Create a user delegation SAS.	Yes
Storage File Data SMB Share Contributor	Allows for read, write, and delete access in Azure Storage file shares over SMB	Yes

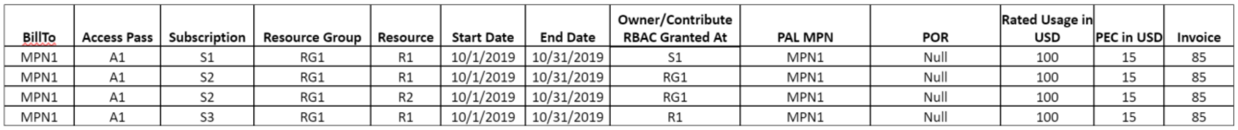
Storage File Data SMB Share Elevated Contributor	Allows for read, write, delete and modify NTFS permission access in Azure Storage file shares over SMB	Yes
Storage File Data SMB Share Reader	Allows for read access to Azure File Share over SMB	No
Storage Queue Data Contributor	Read, write, and delete Azure Storage queues and queue messages. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	Yes
Storage Queue Data Message Processor	Peek, retrieve, and delete a message from an Azure Storage queue. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	Yes
Storage Queue Data Message Sender	Add messages to an Azure Storage queue. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	Yes
Storage Queue Data Reader	Read and list Azure Storage queues and queue messages. To learn which actions are required for a given data operation, see Permissions for calling blob and queue data operations.	No
Support Request Contributor	Lets you create and manage Support requests	Yes

Traffic Manager Contributor	Lets you manage Traffic Manager profiles, but does not let you control who has access to them.	Yes
User Access Administrator	Lets you manage user access to Azure resources.	Yes
Virtual Machine Administrator Login	View Virtual Machines in the portal and login as administrator	Yes
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	Yes
Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.	Yes
Web Plan Contributor	Lets you manage the web plans for websites, but not access to them.	Yes
Website Contributor	Lets you manage websites (not web plans), but not access to them	Yes

b. Appendix B

Partners who purchase Azure Plan from partner center will by default inherit appropriate RBAC access to customer's assets in order to provide 24x7 support. Below table is highlighting some common scenarios that partners could encounter illustrated with examples.

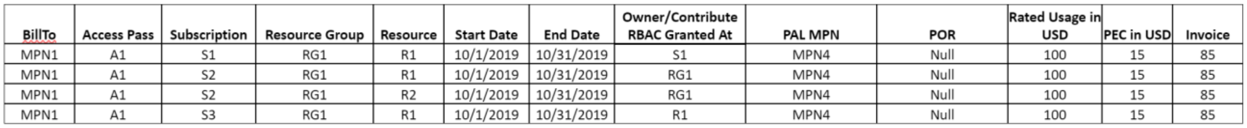
Scenario1 – Direct Partner or Indirect Provider provides 24x7 support for entire billing period



BillTo	Access Pass	Subscription	Resource Group	Resource	Start Date	End Date	Owner/Contribute RBAC Granted At	PAL MPN	POR	Rated Usage in USD	PEC in USD	Invoice
MPN1	A1	S1	RG1	R1	10/1/2019	10/31/2019	S1	MPN1	Null	100	15	85
MPN1	A1	S2	RG1	R1	10/1/2019	10/31/2019	RG1	MPN1	Null	100	15	85
MPN1	A1	S2	RG1	R2	10/1/2019	10/31/2019	RG1	MPN1	Null	100	15	85
MPN1	A1	S3	RG1	R1	10/1/2019	10/31/2019	R1	MPN1	Null	100	15	85

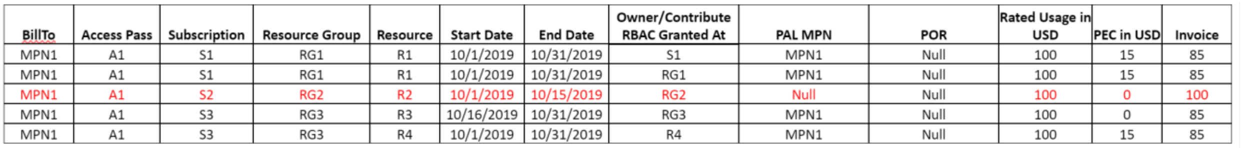
RBAC inherited to the resource and PEC will be calculated for entire period support was provided. Default AOBO will grant necessary RBAC to earn PEC.

Scenario 2 – Transacting Partner or their affiliate manage customer assets (Transact centrally but manage with distributed MPNs)



BillTo	Access Pass	Subscription	Resource Group	Resource	Start Date	End Date	Owner/Contribute RBAC Granted At	PAL MPN	POR	Rated Usage in USD	PEC in USD	Invoice
MPN1	A1	S1	RG1	R1	10/1/2019	10/31/2019	S1	MPN4	Null	100	15	85
MPN1	A1	S2	RG1	R1	10/1/2019	10/31/2019	RG1	MPN4	Null	100	15	85
MPN1	A1	S2	RG1	R2	10/1/2019	10/31/2019	RG1	MPN4	Null	100	15	85
MPN1	A1	S3	RG1	R1	10/1/2019	10/31/2019	R1	MPN4	Null	100	15	85

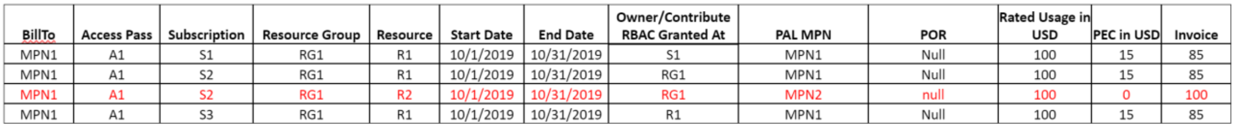
Scenario 3 – Partners partially manage customers assets during the open period of the invoice



BillTo	Access Pass	Subscription	Resource Group	Resource	Start Date	End Date	Owner/Contribute RBAC Granted At	PAL MPN	POR	Rated Usage in USD	PEC in USD	Invoice
MPN1	A1	S1	RG1	R1	10/1/2019	10/31/2019	S1	MPN1	Null	100	15	85
MPN1	A1	S1	RG1	R1	10/1/2019	10/31/2019	RG1	MPN1	Null	100	15	85
MPN1	A1	S2	RG2	R2	10/1/2019	10/15/2019	RG2	Null	Null	100	0	100
MPN1	A1	S3	RG3	R3	10/16/2019	10/31/2019	RG3	MPN1	Null	100	0	85
MPN1	A1	S3	RG3	R4	10/1/2019	10/31/2019	R4	MPN1	Null	100	15	85

Usage for S2 will not get PEC from 10/1 to 10/15 because partner MPN did not have access to customer's azure assets

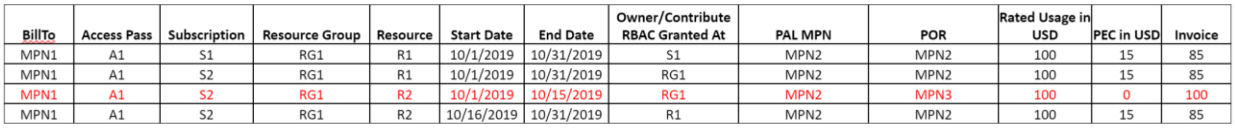
Scenario 4 – MPN agreement associated via Azure portal has expired



BillTo	Access Pass	Subscription	Resource Group	Resource	Start Date	End Date	Owner/Contribute RBAC Granted At	PAL MPN	POR	Rated Usage in USD	PEC in USD	Invoice
MPN1	A1	S1	RG1	R1	10/1/2019	10/31/2019	S1	MPN1	Null	100	15	85
MPN1	A1	S2	RG1	R1	10/1/2019	10/31/2019	RG1	MPN1	Null	100	15	85
MPN1	A1	S2	RG1	R2	10/1/2019	10/31/2019	RG1	MPN2	null	100	0	100
MPN1	A1	S3	RG1	R1	10/1/2019	10/31/2019	R1	MPN1	Null	100	15	85

Usage for S2 will not get PEC because MPN2’s agreement has expired or invalid

Scenario 5 – POR associated in Partner Center and MPN updated in Azure portal does not match



BillTo	Access Pass	Subscription	Resource Group	Resource	Start Date	End Date	Owner/Contribute RBAC Granted At	PAL MPN	POR	Rated Usage in USD	PEC in USD	Invoice
MPN1	A1	S1	RG1	R1	10/1/2019	10/31/2019	S1	MPN2	MPN2	100	15	85
MPN1	A1	S2	RG1	R1	10/1/2019	10/31/2019	RG1	MPN2	MPN2	100	15	85
MPN1	A1	S2	RG1	R2	10/1/2019	10/15/2019	RG1	MPN2	MPN3	100	0	100
MPN1	A1	S2	RG1	R2	10/16/2019	10/31/2019	R1	MPN2	MPN2	100	15	85