Microsoft | MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

CLOUD SUCCESS PLAN FOR AZURE

AZURE MONITOR

Mike McKanna, PMP, ITIL
CSA-E
February 8, 2023

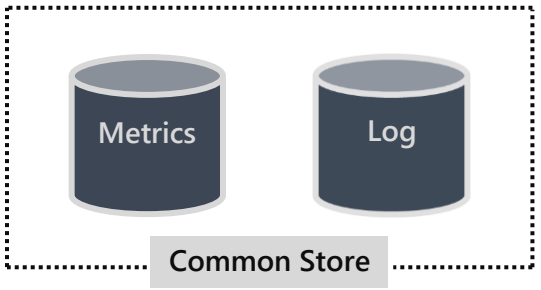
Agenda

- Azure Monitor
- Azure Status
  - Service Health
  - Resource Health
  - Service Incident Overview
  - CritSit Overview
  - Major Incident Preparedness
- Azure Alerts
- Change Management

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

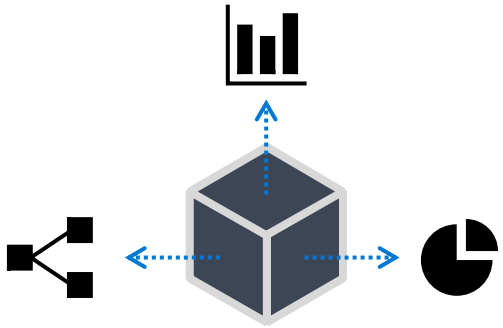
Azure Monitor

Full observability for your infrastructure, applications, network, and more
https://docs.microsoft.com/en-gb/azure/azure-monitor/overview



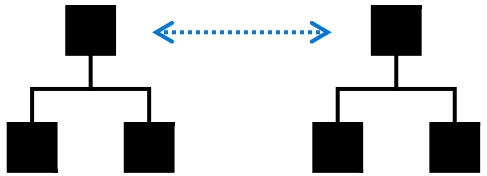
Unified monitoring

A common platform for all metrics, logs and other monitoring telemetry



Data driven insights

Advanced querying and analytics powered by machine learning capabilities

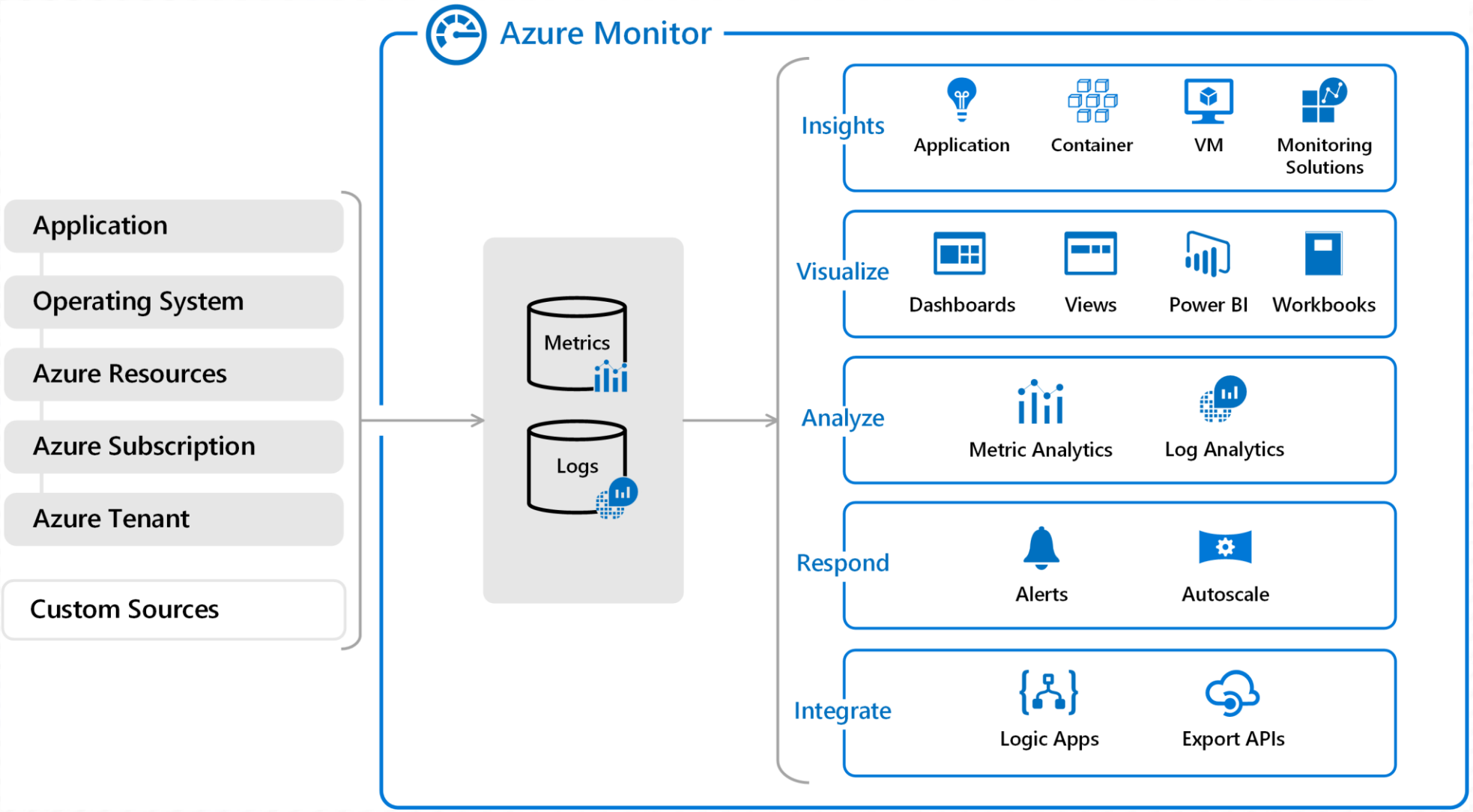


Partner integrations

Rich ecosystem of popular DevOps, issue management, SIEM, and ITSM tools

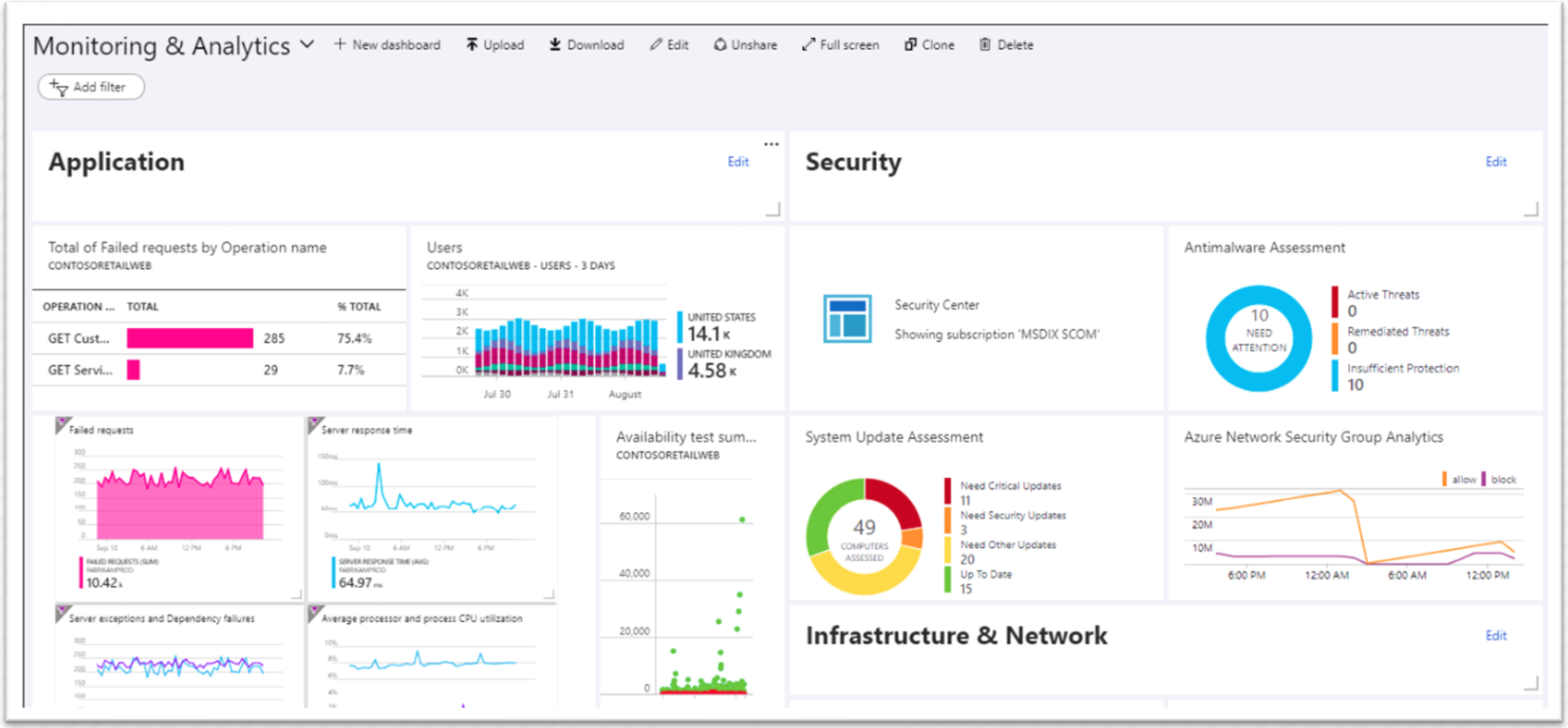
Azure Monitor now includes Log Analytics!

Azure Monitor – Data Platform



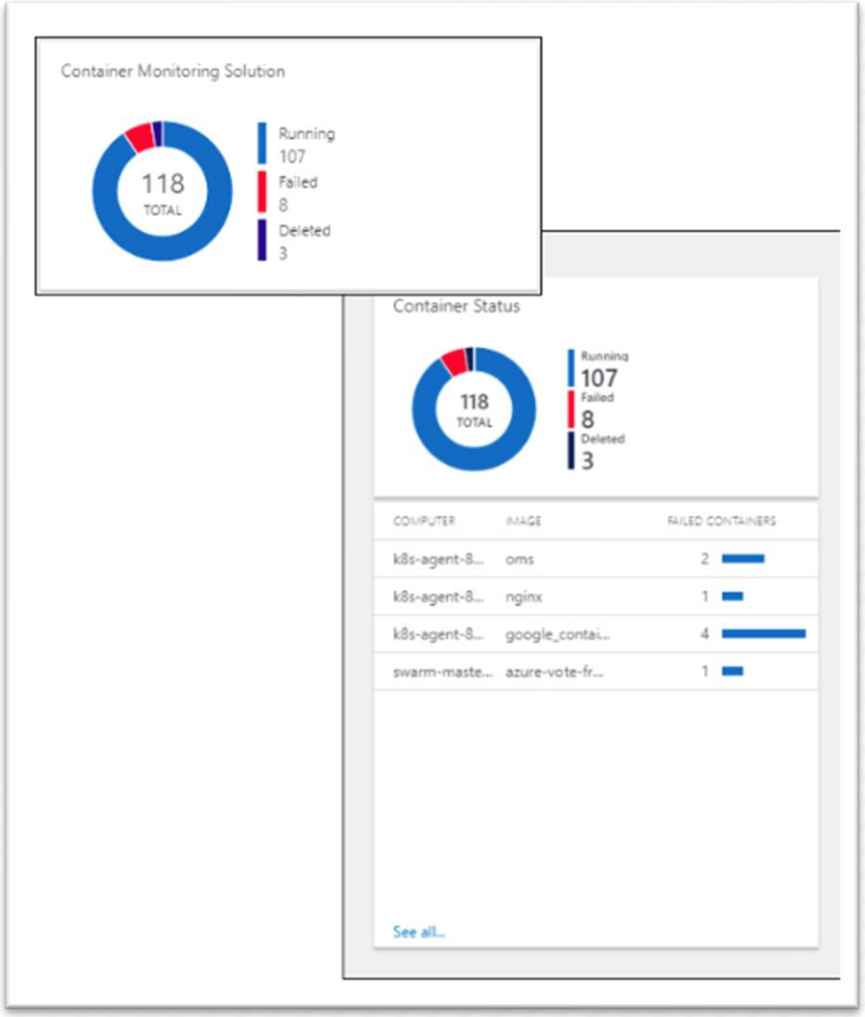
Azure Monitor – Dashboards & Visualization

Azure dashboards allow you to **combine different kinds** of data, including both metrics and logs, into a single pane in the Azure portal. You can **optionally share the dashboard** with other Azure users.



Azure Monitor Views

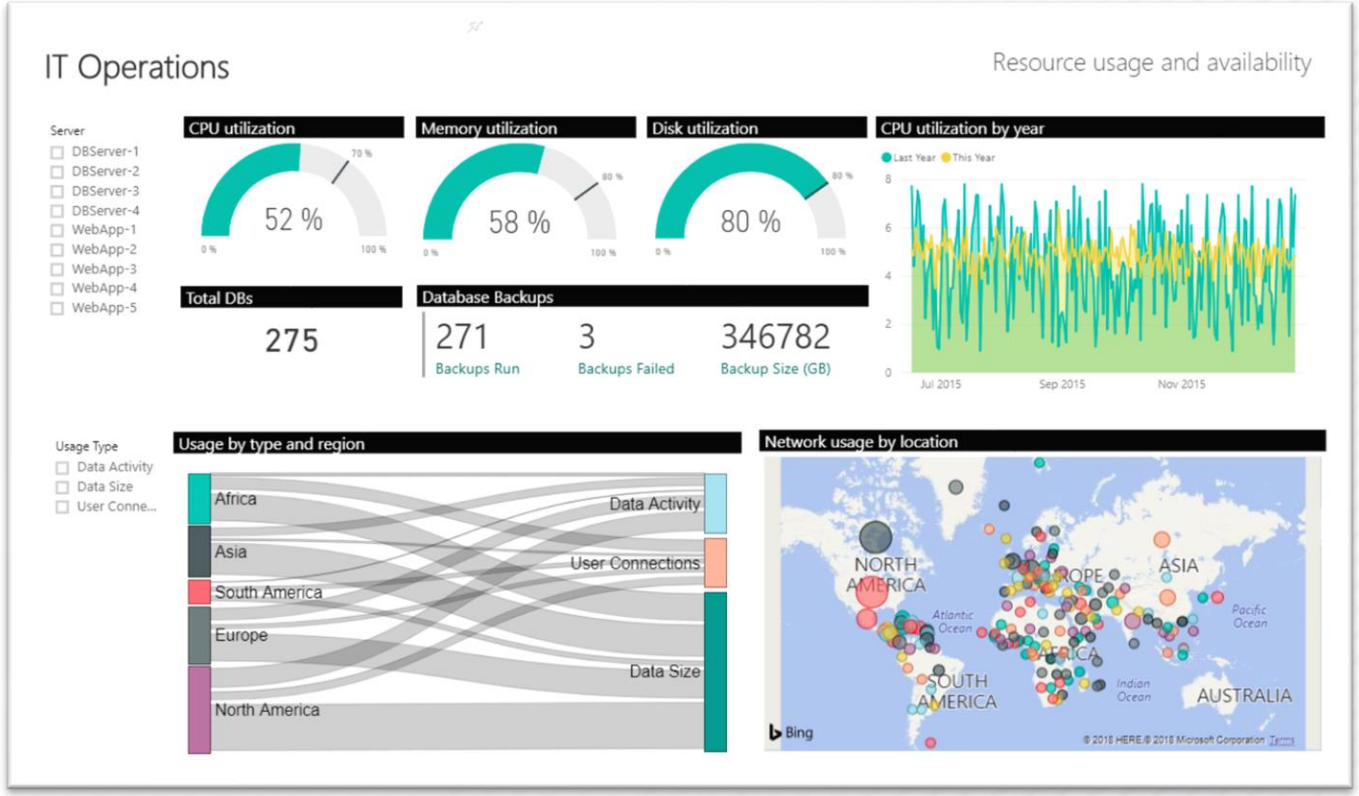
Views visually **present log data** in Azure Monitor. Each view **includes a single tile that drills down to a combination of visualizations** such as bar and line charts in addition to lists summarizing critical data.



Azure Monitor – Power BI

Power BI is a **business analytics service** that provides **interactive visualizations across a variety of data sources** and is an **effective means of making data available to others within and outside your organization**.

You can configure Power BI to **automatically import log data from Azure Monitor** to take advantage of these additional visualizations.



Azure Monitor Integration

It is possible to **integrate Azure Monitor with other systems** and to build **custom solutions** that use your monitoring data. Other Azure services work with Azure Monitor to provide this integration.

Event Hub

- **A streaming platform** and **event ingestion service** that can **transform and store data using** any real-time analytics provider or batching/storage adapters.
- Use Event Hubs to stream **Azure Monitor data to partner SIEM** and monitoring tools.

Logic Apps

- A service that allows you to **automate tasks and business processes** using workflows that **integrate with different systems and services**.
- **Activities are available that read and write metrics and logs in Azure Monitor,** which allows you to build workflows integrating with a variety of other systems

API

- **Multiple APIs** are available to **read and write metrics and logs** to and from Azure Monitor in addition to accessing generated alerts.
- You can also **configure and retrieve alerts.** This provides you with essentially unlimited possibilities to build custom solutions that integrate with Azure Monitor

Azure Status

Service & Resource Health and Incident Management Process

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Azure Service Health

Azure Service Health is a suite of experiences that provide **personalized guidance and support** when issues in Azure services affect you.

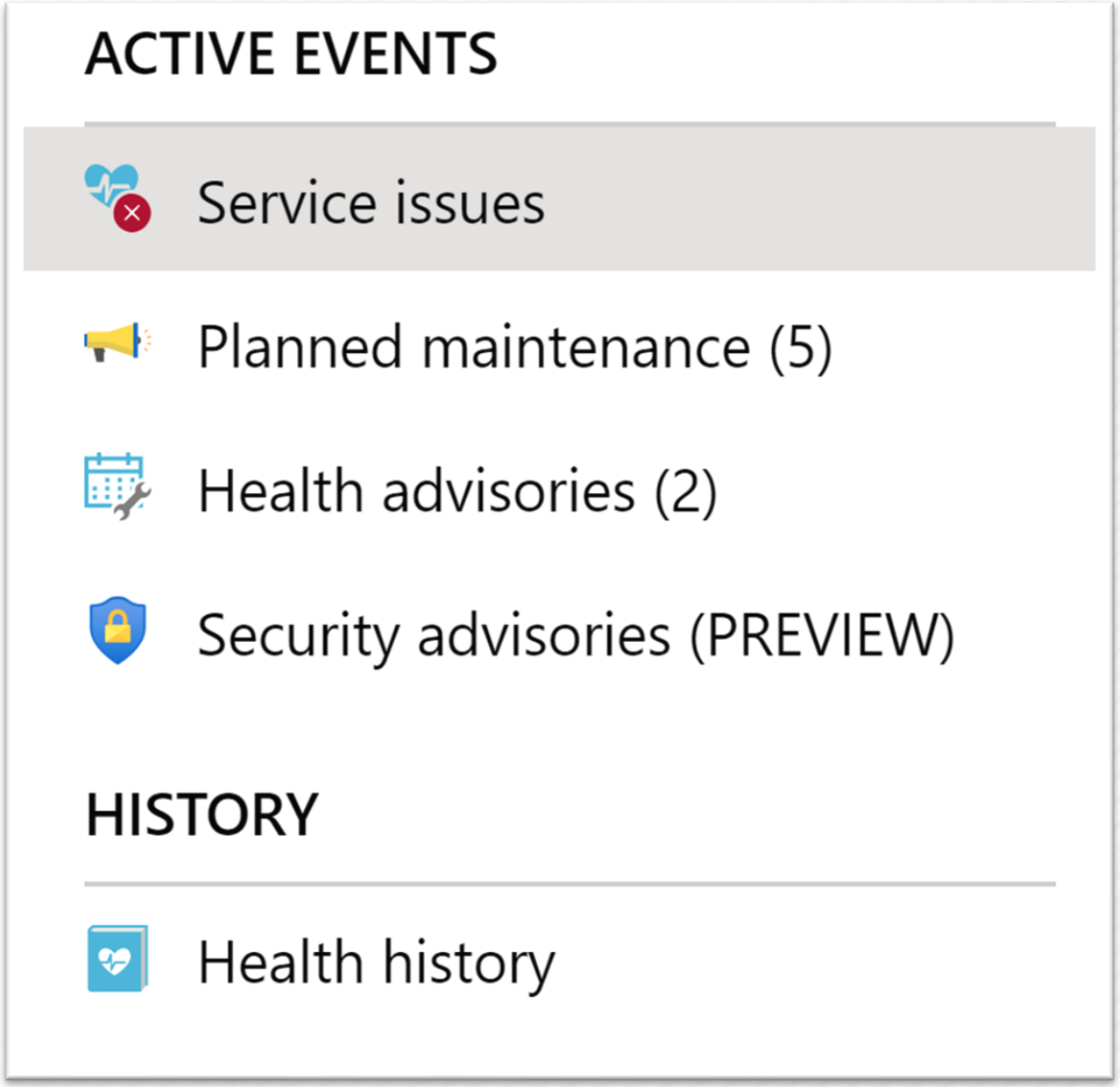
It can **notify you, help you understand the impact of issues**, and keep you updated as the issue resolves.

It can also help you **prepare for planned maintenance** and changes that could affect the availability of your resources.

Service Health

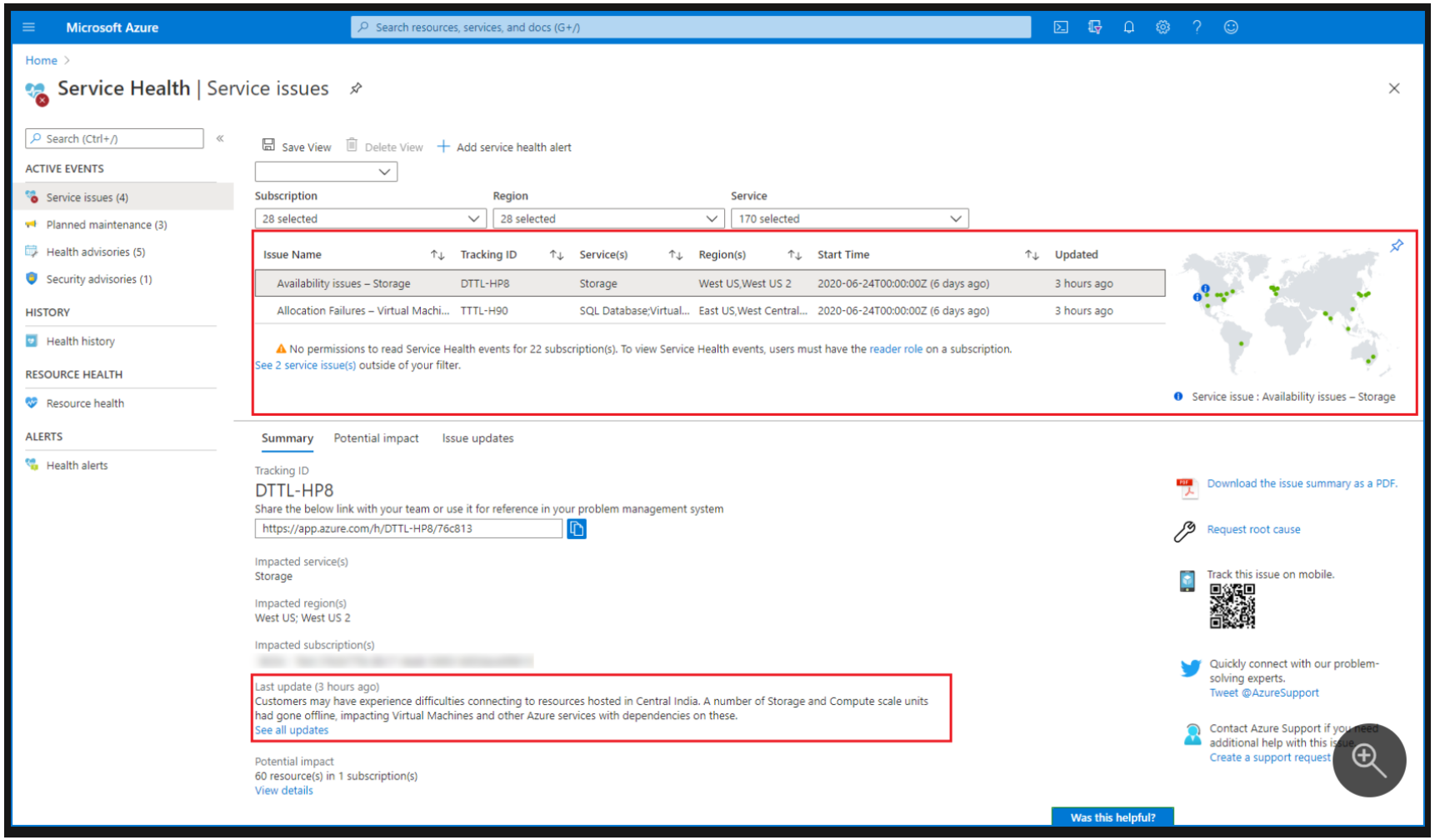
Service Health tracks three types of health events that may impact your resources:

- **Service issues** - Problems in the Azure services that affect you right now.
- **Planned maintenance** - Upcoming maintenance that can affect the availability of your services in the future.
- **Health advisories** - Changes in Azure services that require your attention. Examples include when Azure features are deprecated or if you exceed a usage quota.
- **Health History** - When events become inactive, they get placed in your health history for up to 90 days



Azure Service Health

Service issues dashboard provides real-time insight into Azure service incidents



Administrators can see active incidents or advisories relevant to their tenant(s).

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Azure Service Health

Identify the resources that might be impacted by the issue

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Service Health | Service issues

Search (Ctrl+/)

ACTIVE EVENTS

- Service issues (4)
- Planned maintenance (3)
- Health advisories (5)
- Security advisories (1)

HISTORY

- Health history

RESOURCE HEALTH

- Resource health

ALERTS

- Health alerts

Save View | Delete View | Add service health alert

Subscription: 28 selected | Region: 28 selected | Service: 170 selected

Issue Name	Tracking ID	Service(s)	Region(s)	Start Time	Updated
Availability issues – Storage	DTTL-HP8	Storage	West US,West US 2	2020-06-24T00:00:00Z (6 days ago)	3 hours ago
Allocation Failures – Virtual Machi...	TTTL-H90	SQL Database;Virtual...	East US,West Central...	2020-06-24T00:00:00Z (6 days ago)	3 hours ago

No permissions to read Service Health events for 22 subscription(s). To view Service Health events, users must have the reader role on a subscription.
See 2 service issue(s) outside of your filter.

Service issue : Allocation Failures – Virtual M...

Summary | Potential impact | Issue updates

9 resource(s) in 1 subscription(s) | Export to CSV

Resource Name	Resource Type	Resource Group	Location	Subscription
GangaTFSVM	Virtual machine	ARM-VM-Group	eastus	
casesubtestvm	Virtual machine	casesubmissionuiautomation	westcentralus	
ganeshubuntu	Virtual machine	ganeshtest	eastus	
hcltestdb	SQL database	hcltestrg	westcentralus	
scotthit-testdb	SQL database	scotthit-test	eastus	
scotthit-testdb_2019-03-02t22-34z	SQL database	scotthit-test	eastus	
scotthit-vm2	Virtual machine	vmtest	eastus	
stdescriptions	SQL database	scotthit-test	eastus	
trchetestvm	Virtual machine	trche_test	eastus	

Was this helpful?

Administrators can use the Potential Tab to identify the resources and export the list as a CSV file

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Azure Service Health

See emerging issues which may impact your services

Home > Service Health | Service issues

Service Health | Service issues

Search (Ctrl+/)

Attention - Service issues

ACTIVE EVENTS

Service issues (1)

Planned maintenance (2)

Health advisories

Security advisories (PREVIEW)

HISTORY

Health history

RESOURCE HEALTH

Resource health

ALERTS

Health alerts

1 emerging issue under investigation: Networking Issue in South Central US

Save View | Delete View | Add service health alert

Subscription: 24 selected | Region: 28 selected | Service: 165 selected

Issue Name	Tracking ID	Service(s)	Region(s)	Start Time
Application Insights - Multiple regions - Applying Mitigat...	PT_ZZ-470	Virtual Machines	West Europe	2020-02-26T20:0

No permissions to read Service Health events for 3 subscription(s). To view Service Health events, users must have the reader role on a subscription.

Summary | Potential impact | Issue updates

Tracking ID
PT_ZZ-470
Share the below link with your team or use it for reference in your problem management system
https://app.azure.com/h/PT_ZZ-470/497ff9

Impacted service(s)
Virtual Machines

Impacted region(s)
West Europe

Impacted subscription(s)
EngSys Supportability - Test Env (4970d23e-ed41-4670-9c19-02a1d2808ff9)

Last update (2 days ago)
Starting at 14:53 UTC on 21 Feb 2020 you have been identified as a customer using Application Insights who may be experiencing intermittent data latency, d
alert activation. Engineers are aware of this issue and are applying mitigation. The next update will be provided in 60 minutes, or as events warrant.
See all updates

Potential impact
0 resource(s) in 1 subscription(s)
View details

Emerging issues
1 issue

Networking Issue in South Central US

Starting at 12:48 UTC on 28 Feb 2020 a subset of customers in South Central US may encounter failure notifications when performing service management operations on resources hosted in this region. Engineers are aware of this issue and investigating. The next update will be provided in 60 minutes, or as events warrant.

Frequently asked questions

Is this incident impacting me?

Engineering teams are investigating an emerging issue and working to confirm if this incident impacts you. If we confirm that you are impacted, you will receive regular updates throughAzure Service Health.

Can I set up alerts to get informed about this incident?

You can set up Service Health alerts to receive notifications about this incident. You will only receive notifications if we confirm that this incident impacts you. Visit aka.ms/ash-alerts for instructions on how to set up Service Health alerts.

Please note that Service Health alerts won't notify you about emerging issues until we confirm that you are impacted. However, if you want to be notified about emerging issues where you haven't yet been confirmed as an impacted customer, you can consume the RSS feed from the Azure Status Page.

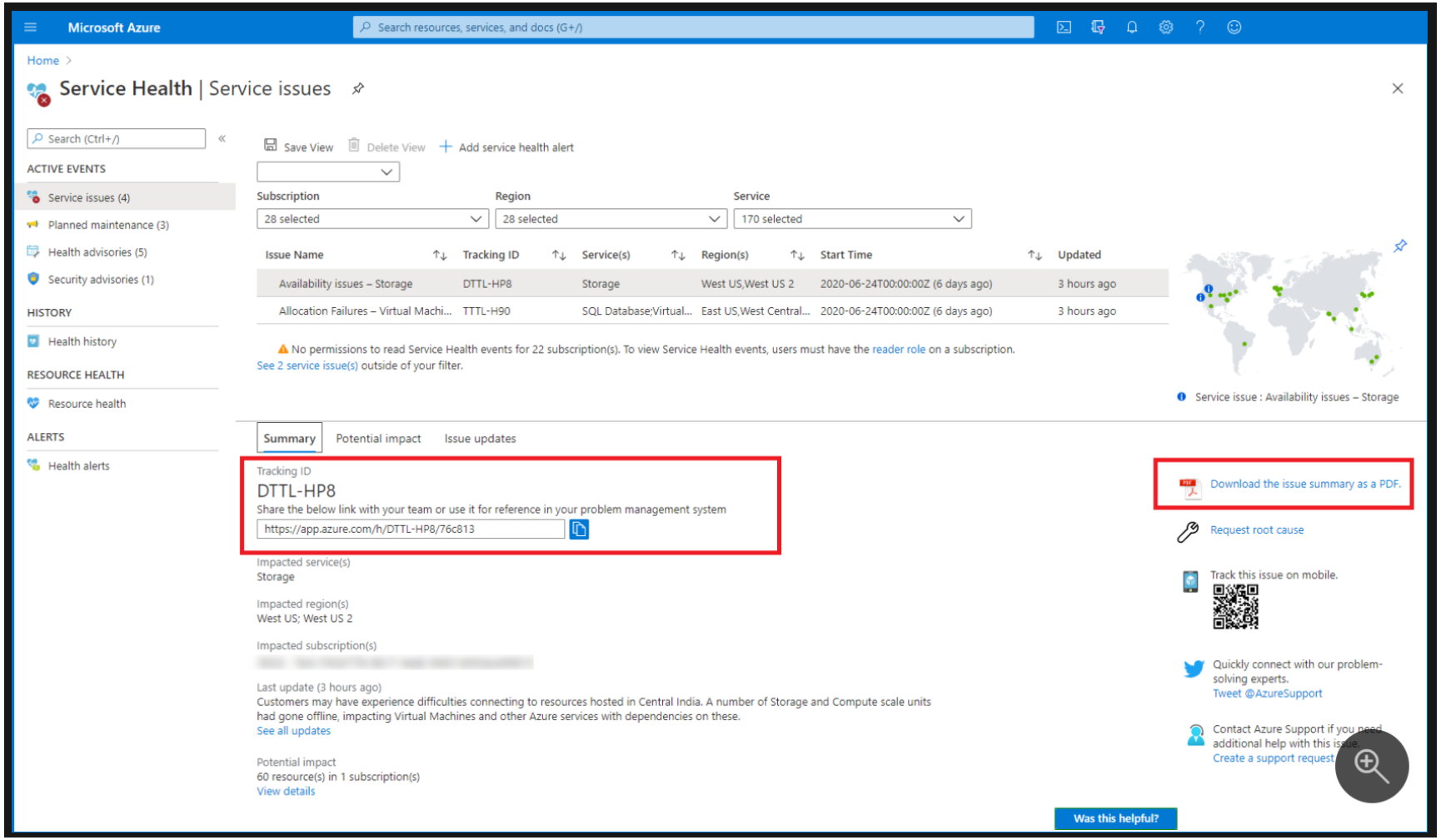
Why am I seeing this?

Receiving this notification doesn't necessarily mean you are impacted. Azure aims to be very transparent regarding any issue that may be impacting you. We understand that you have critical operations that depend on our cloud and could notice an impact before we confirm that you are affected. Visit Azure Service Health to learn more about issues that may be impacting your Azure services and regions.

Administrators can use emerging issues to mitigate widespread services issues that may be posted to the Azure Status page before target communications can be sent to impacted customers.

Azure Service Health

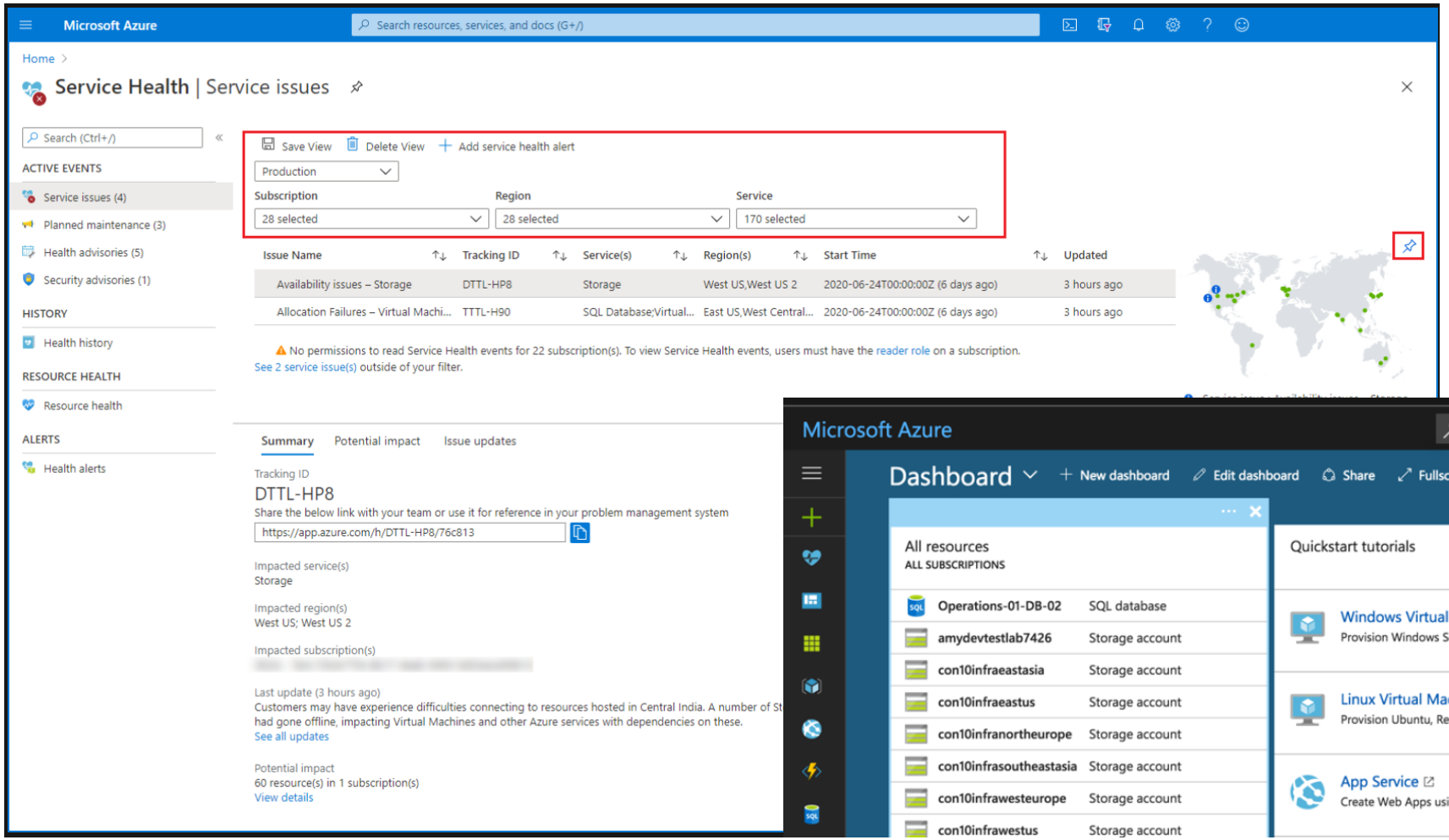
Get links and downloadable explanations



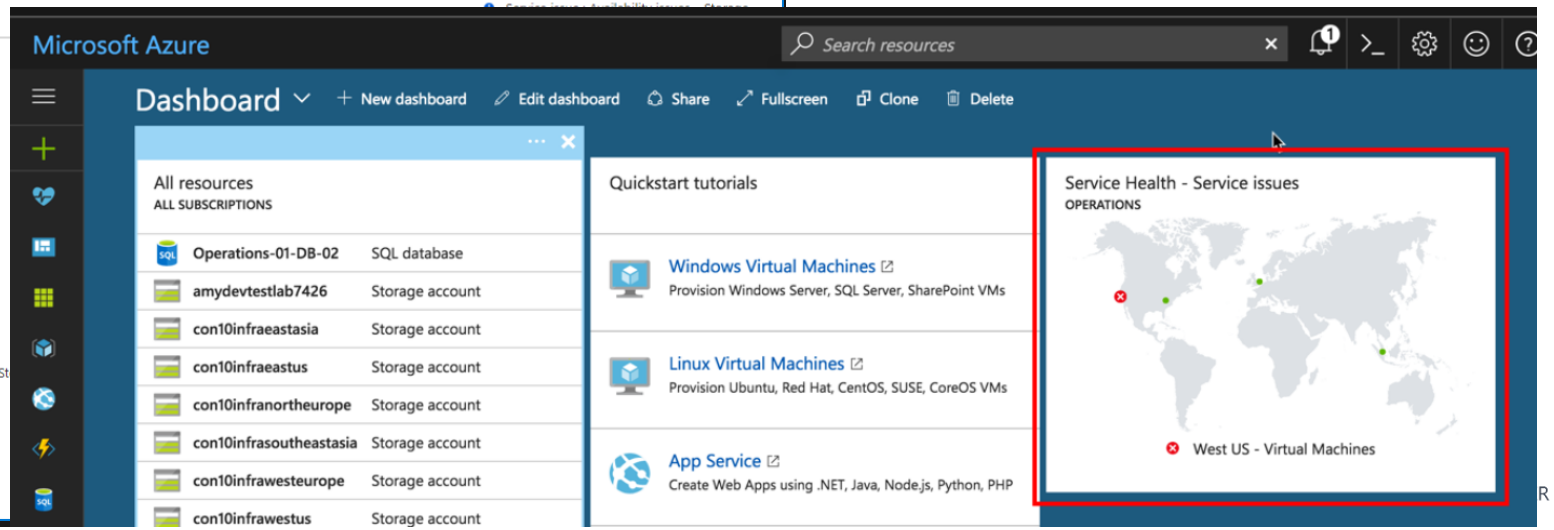
Administrators can create a link for the issue to use in you problem management system, download PDF and sometimes CSV files to share with stakeholders that don't have access to the Azure Portal

Azure Service Health

Pin a personalized health map to your dashboard

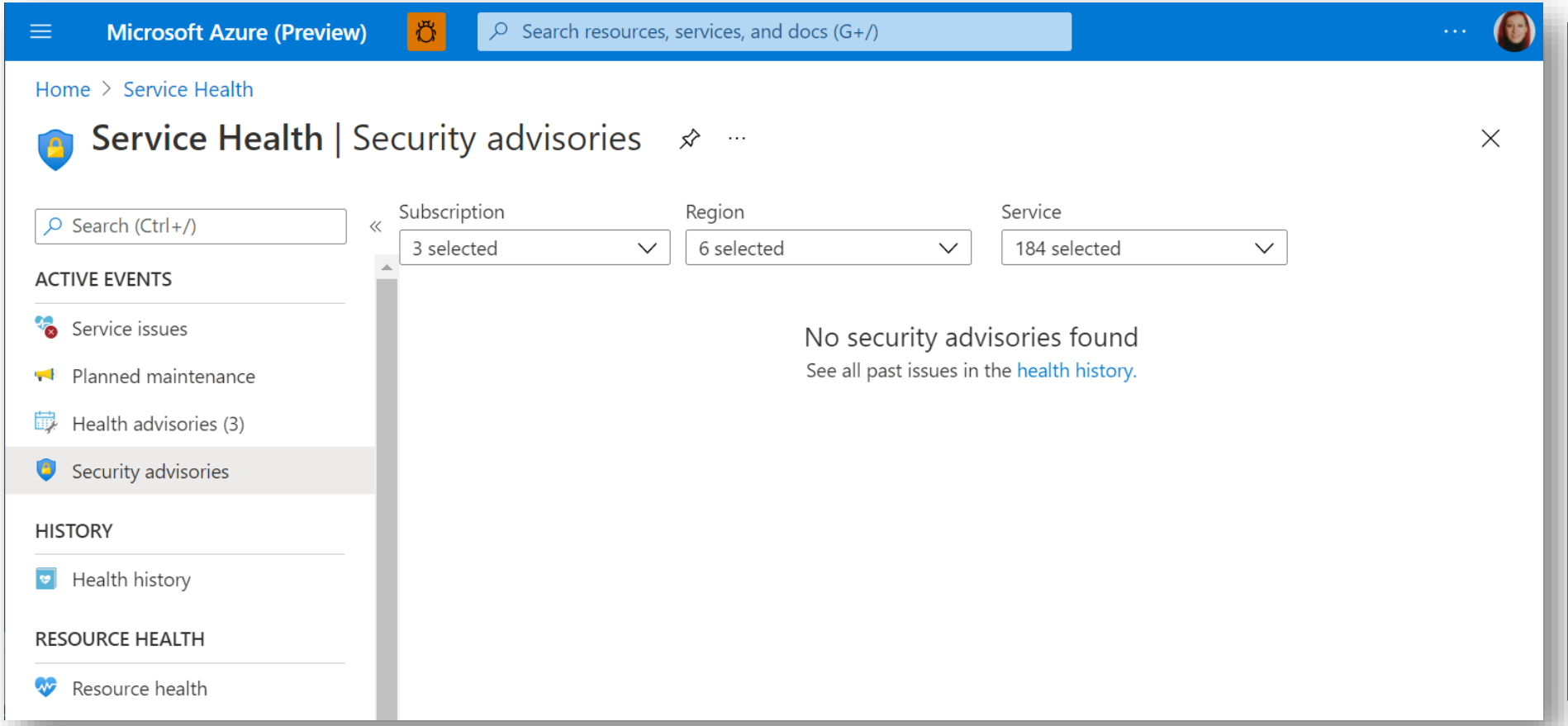


Administrators can filter Service Health to show your business-critical subscriptions, regions and resources types



Azure Service Health > Security advisories

Notifications that communicate urgent security-related information affecting your Azure workloads



- Available since April 2020
- Not to be confused with Azure Advisor, Azure Security Center or Azure Sentinel
- **Security advisories** blade shows security and privacy breaches **at Azure service level**

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Service Incident

What exactly is a “service incident”?

Service incident is the term that Microsoft uses to refer to an event (or series of events) that typically causes multiple customers to have a degraded experience with one or more of our services

These incidents are effectively platform issues that cause **unplanned downtime** – including

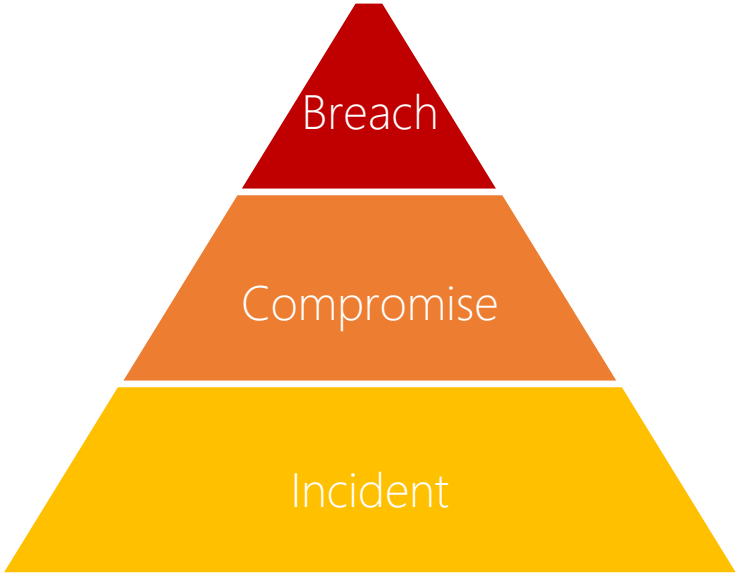
- Unavailability.
- Performance degradation impacting users.
- Problems interfering with service administration or management.
- Security related or violation that may affect Azure Services availability.

When an Azure incident is declared, **we send updates** to all impacted tenants to provide visibility and relevant guidance.

Cyber Security Service Incident

What exactly is a “Cyber Security service incident”?

A **security incident** is an event that affects the **confidentiality, integrity, or availability** of information resources and assets in the organization.



Incident ≠ Compromise ≠ Breach

Breach – We have confirmation that vital information has left the organization.

Compromise - Something bad happened to the confidentiality, integrity, or availability of information resources and assets in the organization.

Incident – Something happened.

What if I have a Cyber-Security Incident?

CSS

- Customer - Call 800-936-3100 to open a Severity A support case
- First point of contact for all security incidents
- Remote investigation of target machines and environments
- Deep technical expertise

Detection and Response Team

- Onsite Incident Response support for targeted attacks or advanced persistent threats
- Broad investigation of customer's entire enterprise
- Determine scope of compromise for follow-on activity

CE

- Onsite support for system rebuilds following destructive attacks*

Limited availability by region

MCS

- Compromise Recovery *following* an investigation (via Detection and Response Team or 3rd party)
- Long-term strategic recovery, modernization, and hardening

Service Incident Communication Model

- When a service incident occurs, Microsoft recognizes that timely, targeted, and accurate communications are critical for customers.
- Microsoft notifies administrators by updating the Service Health blade on the Azure Portal.
- Service incident updates are typically provided on an hourly cadence or, if a different cadence is required, it will be stated in the SHD communication posting.

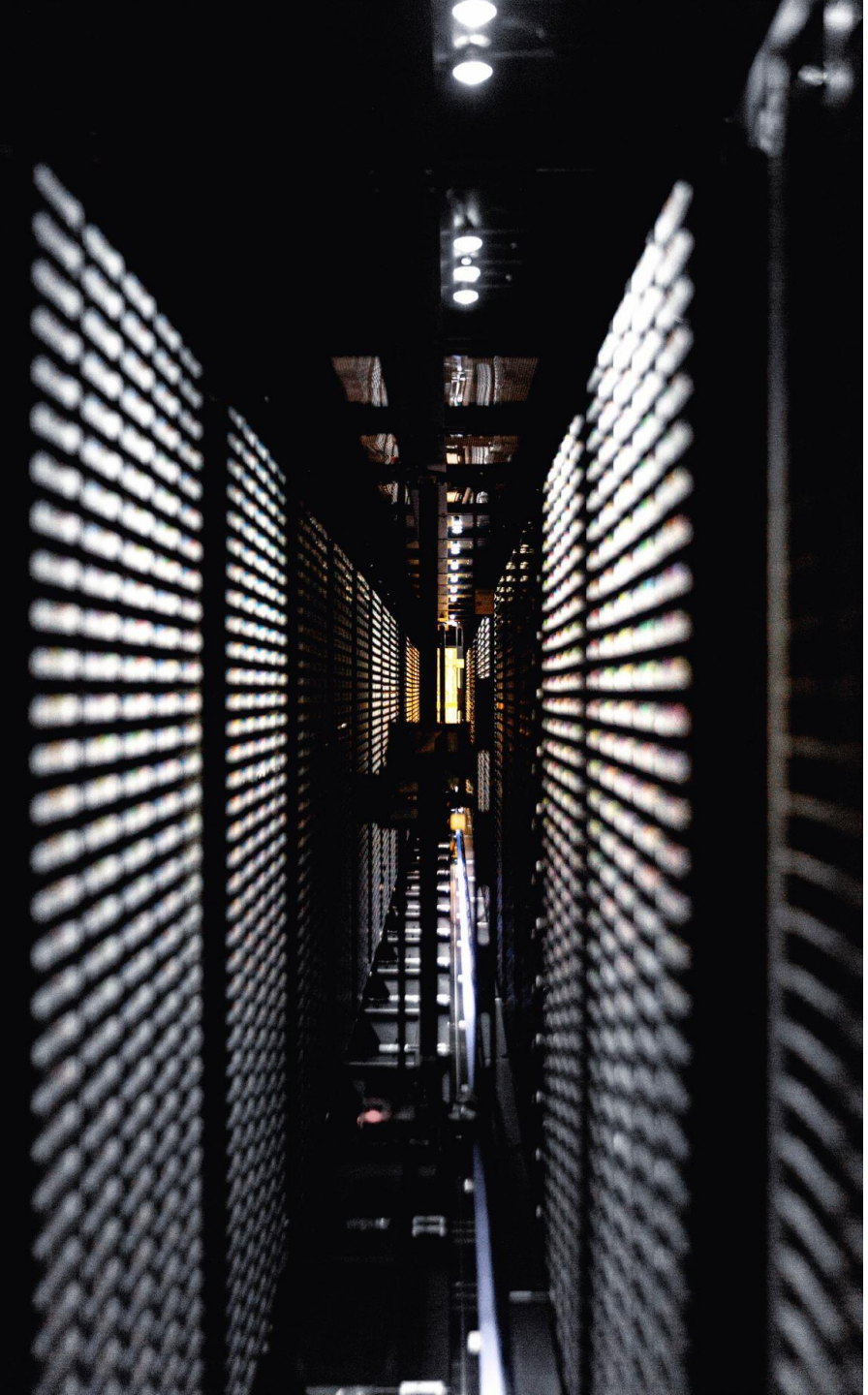
Starting at 23:55 UTC on 11 Nov 2020, you were identified as a customer using Azure Active Directory through the management portal who may experience failures while using the Bulk operations feature. Re-trys will not be successful until the incident is mitigated. Customers may use the portal for single operations as a work-around at this time.

Current status: We have identified a preliminary root cause and are actively applying mitigation steps. The next update will be provided in 60 minutes, or as events warrant.

(4 weeks ago)

Starting at 23:55 UTC on 11 Nov 2020, you were identified as a customer using Azure Active Directory through the management portal who may experience failures while using the Bulk operations feature. Re-try will not be successful until the incident is mitigated. Customers may use the portal for single operations as a work-around at this time.

Current status: We are aware of this issue and are investigating. The next update will be provided in 60 minutes, or as events warrant.



Our communications philosophy

The five pillars

Speed
Is it me or is it Azure?

Accuracy
Which of my resources are impacted?

Discoverability
How can I be notified proactively?

Parity
How can I standardize operations across services?

Transparency
What really happened?

Critical Situation (CritSit) Unified

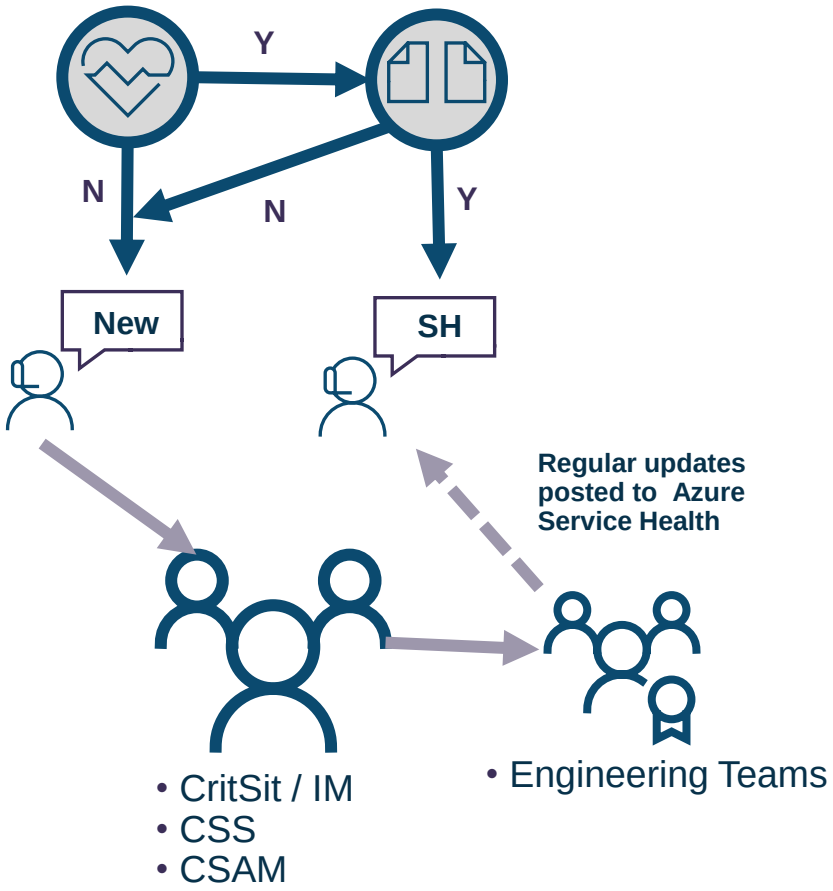
Severity and situation	Our Expected Response	Your Expected Response
Critical Business Impact: • Loss of a core business process and work cannot reasonably continue • Needs attention within 30 minutes	• First call response in 30 minutes or less • Critical situation resource assigned in 30 minutes or less • Resources at your site, after 24 hours, with customer agreement • Continuous effort on a 24x7 basis • Access to Microsoft's experienced specialists and rapid escalation within Microsoft to product teams • Notification of our senior executives, as required	• Appropriate communication with your senior executives, as requested by us • Allocation of appropriate resources to sustain continuous effort on a 24x7 basis • Rapid access and response

For critical business impact severity incidents, an enhanced escalation process is initiated and automatically executed for Performance Support

The assigned Microsoft resource is then responsible for ensuring continued technical progress by providing you with status updates and an action plan

In the case of a Service Incident, Critical business impact **communications will follow the Service Incident communications model**

Major Incident Process



STEPS

Check Service Health Blade

N
Y/N
Y/Y

If there is no mention of the incident, *open a new incident*
If the incident is mentioned, compare the symptoms
If your symptoms do not match, *open a new incident*
If the symptoms match, open a ticket referencing the *SH ID*

- CritSit and CSS are activated; CSAM is notified

  Regular updates posted to Service Health Blade

- First point of technical support with screened US Person in US Location
- Support-related customer-provided files stored "in boundary"
- Engineering Teams engaged; customer consent required to include other non-US Person/US Location Support Engineers

  Solution posted to Service Health Blade

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Azure Service Health & Support Cases

Service Health

Why should I use Service Health instead of status.azure.com?

Many customers check status.azure.com at the first signs of potential issues, to see if there are known issues on the Azure platform at the time. This page shows widespread issues but doesn't show smaller incidents that impact fewer customers.

Azure Service Health (within the Azure portal) knows which subscriptions you manage, so it shows a much more accurate view of any known issues impacting your resources. It also lets you configure health alerts, to find out about any issues through your preferred communication channel(s) – email, SMS, webhook, etc.

Support Case

When do I need to open a Microsoft support case?

During an active incident, many customers and partners contact support (or their account teams) asking for information – but all the details about an active incident, including the latest updates, are available in the Service Health dashboard and through its health alerts.

Customers can and should contact Microsoft support to troubleshoot issues that don't match the impact described in Service Health, but don't need to contact support just for updates. This way, support engineers are available to assist customers with failover activities, or to help with any unrelated but urgent issues.

Consider using the Azure Support REST API for automation and tolling integration.

Microsoft Major Incident Teams

CritSit

Critical Situation Management Team

Automatically notified and engaged

- Reviews and documents business impact with your team
- Advocates for you within Microsoft
- Partners with engineering teams to ensure technical resources are engaged
- Provides executive summaries at initial engagements and increments based on your support level
- Facilitates the dispatch of a Premier Field Engineer to your location for assistance if needed
- Advises you of new contact and performs detailed hand-off if there is shift end for your CritSit manager

CSS

Customer Service & Support

Partner with CritSit

- Assigns a technical support owner
- Commits the best resources
- Establishes a clear action plan
- Escalates as required

How to Stay Informed

Before an incident

1. Optimize the reliability of critical workloads using the Well-Architected Framework and Review.
2. Get familiar with Azure Service Health in the Azure portal – your ‘go to’ place in case of issues.
3. Configure Service Health alerts to notify you about any issues – by email, SMS, webhook, etc.
4. Consider Resource Health alerts or Scheduled Events to inform you of resource-specific issues.

During an incident

1. Review **Azure Service Health** within the Azure portal for the latest updates from our engineers.
2. If there are issues accessing Service Health or the portal itself, check the public **Azure Status page**.
3. If there are ever issues with the Status page, check for any updates via **@AzureSupport** on Twitter.
4. If your impact/issues don’t match the incident (or if these persist after mitigation) **contact support**.

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

All cases must be opened in the Azure portal

Please ensure that all “case creators” have at least the Support Request Contributor role

Global Administrator
Owner (Azure RBAC)
Contributor (Azure RBAC)

Accesses all administrative features (per role) in the Azure portal including access to create support requests.

Support Request Contributor

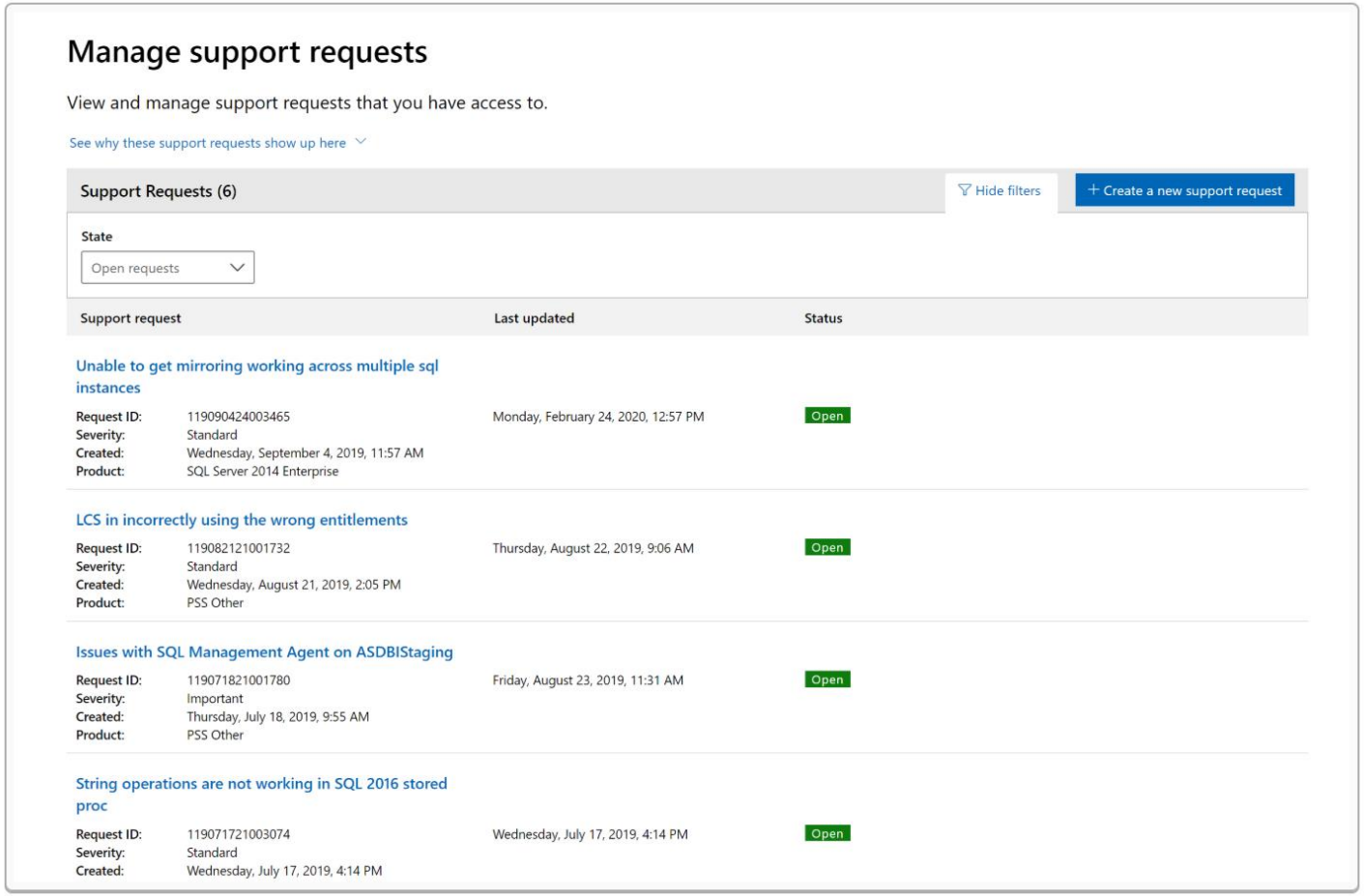
Creates and manages support requests and has view only permissions for Service Health. Assigned at the subscription level.

Click here for more information

MS FEDERAL
CLOUD & CUSTOMER EXPERIENCE TEAM

Manage Support Requests via Services Hub

Login here to access this functionality:



Support Request Status in Services Hub

- Provides more information at-a-glance for each Support Request including status, and specifications.
- This information is available without the need to click through or expand the selection for a more intuitive and simplified experience.

Note: User Interface changes occur to improve your experience

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Root Cause Analysis

For significant incidents with broad service impact

Available within 3 business days

Published to Service Health

Review with Customer by CSAM

Contents

Incident Information & Summary
What happened and why?

Customer Impact
What was the effect?

Incident Timeline
Start Date & Time
End Date & Time

Root Cause
Why did it happen?

Next Steps
How can we prevent it in the future?

Service Incident Communication

Primary Channels
Channels

Additional

Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
jdoe@contoso.com
Contoso

Home >

Service Health | Service issues

Search (Ctrl+/)

ACTIVE EVENTS
- Service issues
- Planned maintenance
- Health advisories (1)
- Security advisories

HISTORY
- Health history

RESOURCE HEALTH
- Resource health

ALERTS
- Health alerts

Save View | Delete View | Add service health alert

Subscription: 12 selected
Region: 5 selected
Service: 183 selected

4:56 — Notifications

TODAY
- Active: Virtual Machines - East... 10:12 AM
  Starting at 07:43 UTC on 10 Nov 2017, you hav...

WEDNESDAY
- Resolved: Virtual Network - Ea... 2:56 PM
  SUMMARY OF IMPACT: Between 21:26 and 22:11 UTC on 15 Nov 2017, you were identified as a customer in East US who may have received fai...
- Resolved: We have important i... 10:01 AM
  As a final reminder, the new .NET Framework 4.7.1 version is scheduled to gradually deploy to Azure App Service during December 2017. Azur...

SUNDAY
- Resolved: Virtual Machines - K... 6:39 AM
  subs not specified sending again

4:54 — BetaMaster, Virtual machine

Metrics
- Disk read and write
- Network in and out

Resources
Extensions
Properties

Microsoft Azure — My account — Portal

Azure status
Updated 27 seconds ago
RSS

View other issues that might be impacting your services:
Go to Azure Service Health

HELPFUL LINKS
- Azure status history
- Get notified of outages that impact you
- Building reliable applications on Azure

Refresh every: 2 minutes

Good | Information | Warning | Critical

Americas | Europe | Asia Pacific | Middle East and Africa | Azure Government | Azure China

PRODUCTS AND SERVICES | *NON-REGIONAL | EAST US | EAST US 2 | CENTRAL US | NORTH CENTRAL US | SOUTH CENTRAL US | WEST CENTRAL US | WEST US | WEST US 2 | CANADA EAST | CANADA CENTRAL | BRAZIL SOUTH | BRAZIL SOUTHEAST

COMPUTE
- Azure VMware Solution by CloudSimple
- Virtual Machines
- SAP HANA on Azure Large Instances
- Windows Virtual Desktop
- Virtual Machine Scale Sets

Explore
Settings

Azure Support
164.9K Tweets

Microsoft
Your gateway to Azure support, across the globe

Follow

Azure Support
@AzureSupport
Official Microsoft Azure account for improving the customer experience by connecting the Azure community to the right resources - answers, support, and experts.
status.azure.com | Joined April 2015
802 Following | 66.9K Followers

Tweets | Tweets & replies | Media | Likes

Alerts

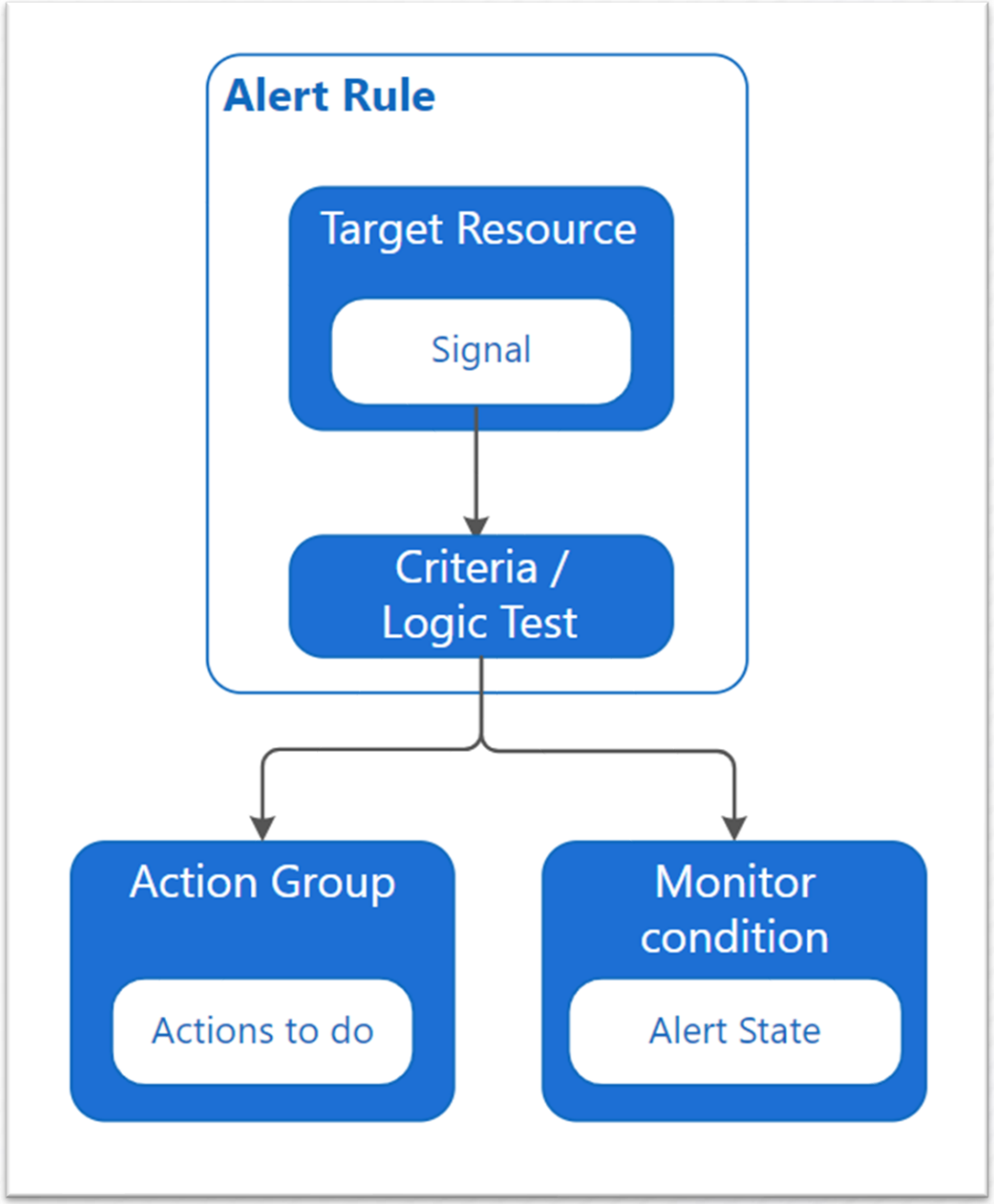
Define metrics and actions to be aware overall cloud health

Alerts

Alerts **proactively notify** you when **important conditions** are found in your monitoring data. They allow you to identify and address issues before the users of your system notice them.

Alerts should be **converted to actionable items** e.g. trigger governance discipline, incidents, problems or change requests

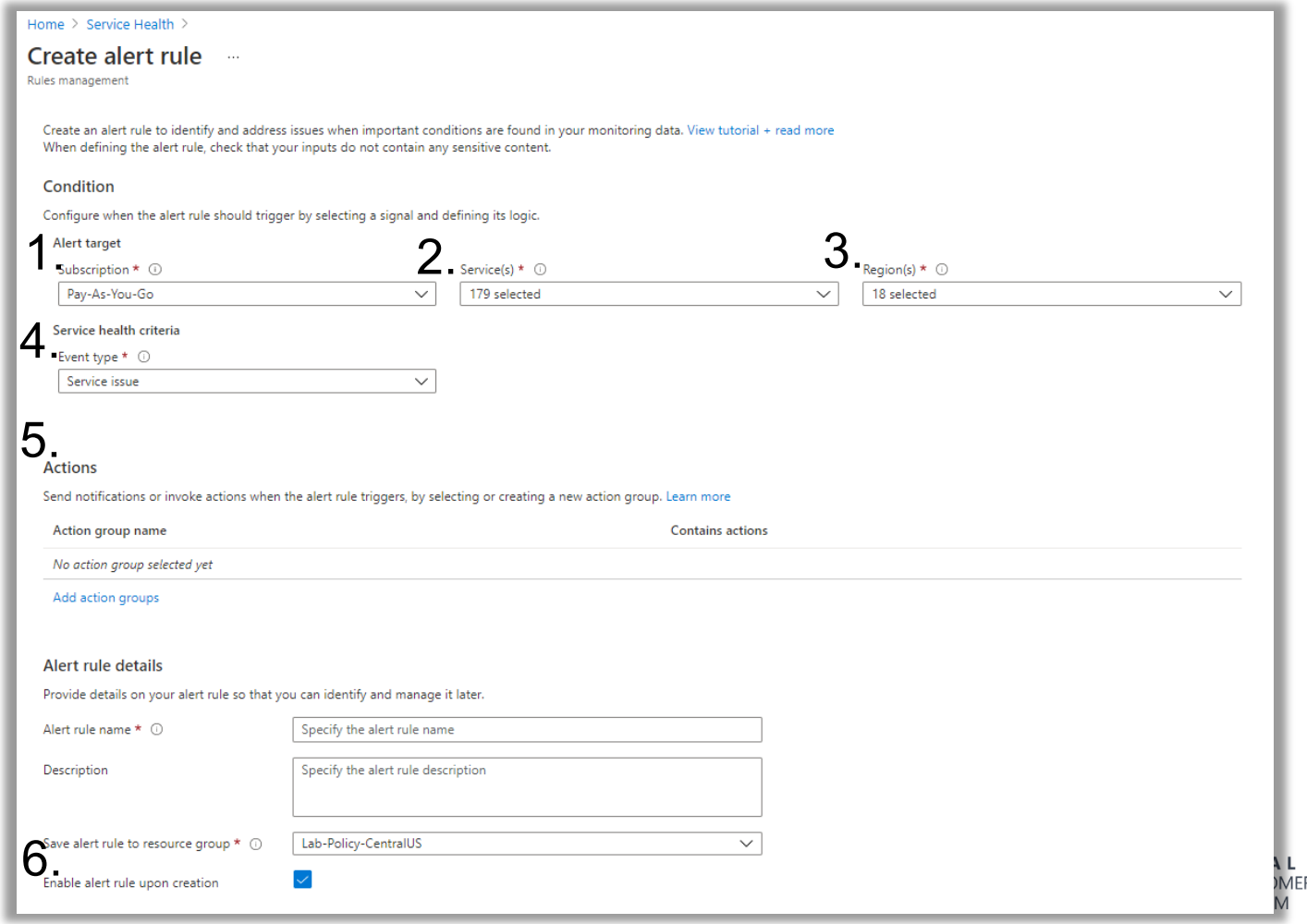
Azure Alerts



Azure Service Health Alerts

Monitor Service Health by Creating Alert Rules

1. Select Subscription
2. Select service(s) to include
3. Select regions to include
4. Select Event Type(s):
   - Service Issue
   - Planned Maintenance
   - Health Advisories
   - Security Advisories
5. Send notifications or invoke actions when the rule triggers
6. Enable the Alert Rule

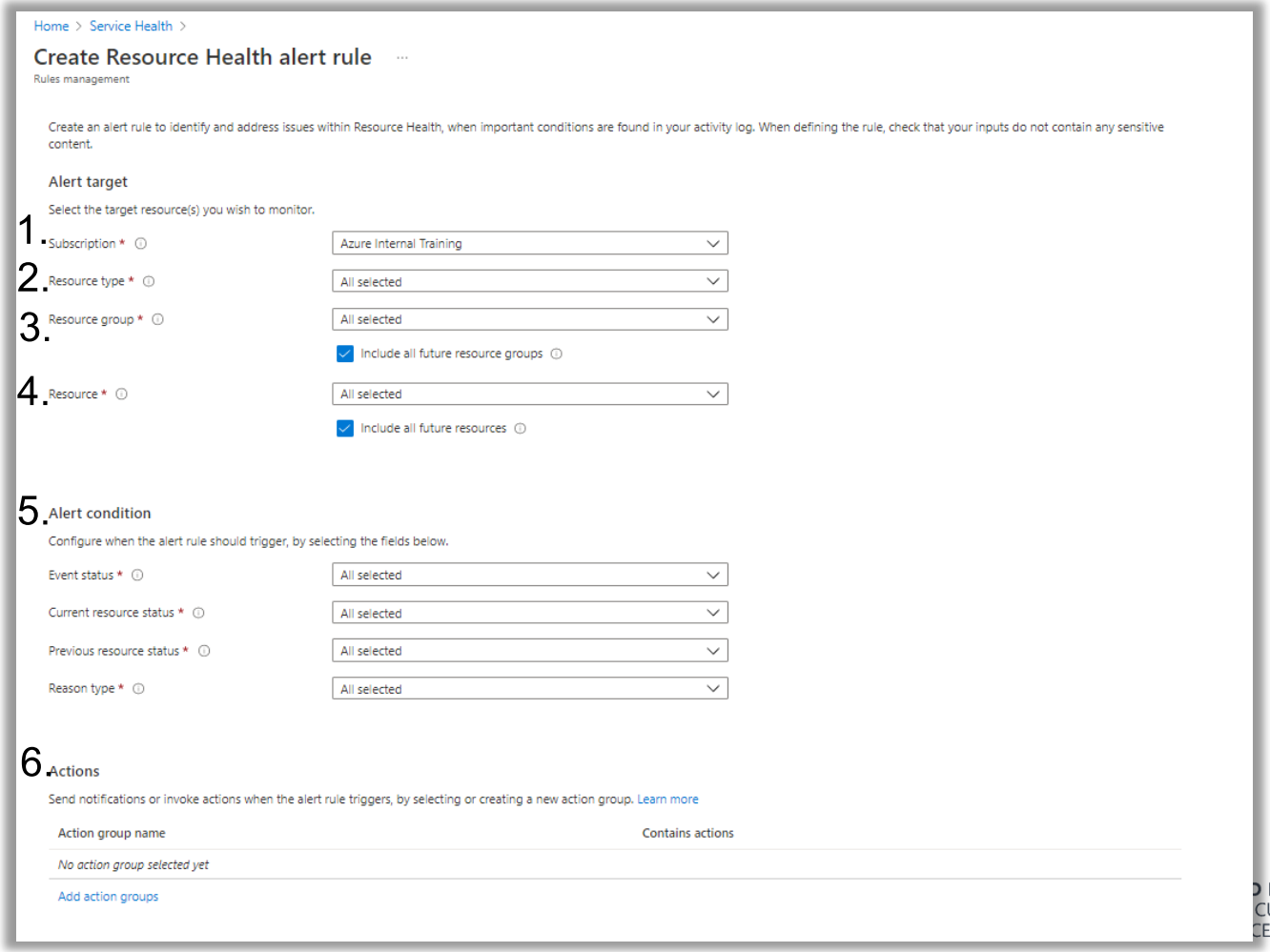


Configure notifications
Configure actions

Azure Resource Health Alerts

Monitor Resource Health by Creating Alert Rules

1. Select Subscription
2. Select resource type(s) to include
3. Select resource group(s) to include:
4. Select resource(s) to include
5. Set Alert Conditions
6. Send notifications or invoke actions when the rule triggers



[Configure notifications]
[Configure actions]

Azure Service Health – Alerting Strategy

How to develop your service health altering strategy for your team:

1. Think about *criticality*. How important is a given subscription, service, or region? If it's production, you'll want to set up an alert for it, but dev/testing might be unnecessary.
2. Decide *whom to inform* in the event of an issue. Who is the right person or team to tell about a service issue so they can act? For example, send Azure SQL or Azure Cosmos DB issues to your database team.
3. Finally, agree on *how to inform* that individual or team. What is the right communication channel for the message? Email is noisy, so it might take longer for your teams to respond.

Major Incident Response Plan

Communications and data required to stay informed

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Critical Situation Timeline

Premier/Unified Support

0-1 Hour

Qualification

Microsoft CritSit manager identified; remains end-to-end

Business and technical scope impact

Account team awareness and engagement

1-4 Hour

Depth technical resource introduction

Early Business Scope

6 Hours

Every 6 Hours

Power Triage

CritSit manager led

Escalation Services to required groups as needed

Regular Executive Summaries

Relief Point

Incident insights recorded

Summary at Close

5 Business Days

Service Management Review

Risk assessment and remediation – leveraging insights

Review Led By CSAM

End-to-End Ownership

*Please see your service description at contract sign date. Link to Service Description: https://enterprise.microsoft.com/en-us/services/support-consulting-services-description/)

Premier/Unified Support

Major Incident Response Plan

Reactive Support Information at a Glance

Support Contract

Duration:

DD MMM YYYY

DD MMM YYYY

Your Support Team

Your Customer Success Account Manager

Firstname Lastname

321-654-0987

User.name@microsoft.com

CSAMs Manager

Givenname Surname

789-456-1230

Csam.mgr.name@microsoft.com

Incident Manager

Person Family

alias@Microsoft.com

Reactive Support

Support (24x7)

- **1 hour for Sev 1 & Sev A (Critical) issues**

Incident Status

https://portal.azure.com

http://support.microsoft.com/premier

Premier PubSec Support Hotline

(855) 255-3054; Intl collect (206) 802-6689

Service Admin Name and Contact information:

Customer Person, custpers@custdom.com

Stakeholder Contact Information

CUSTOMER				
Name	Access ID	Title	Phone	Email
		Azure Service Owner		
		Incident Management Lead		
		Cloud Application Lead		
		Technical Architect(s)		
		Service Desk Lead		

MICROSOFT			
Name	Title	Phone	Email
	Customer Success Account Manager	Use Mobile	
	CSAM Manager	Use Mobile	
	Incident Manager	Use Support	
	Account Technology Strategist	Use Mobile	

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Key Tenant Information

Azure

Key Info	
Subscription ID (Can be found on Azure Portal)	<ID>

Do Not collect classified ID

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Email Communications to Customer

Initial & Update	Update Only	Customer Incident
First Notification and all Ongoing Updates All communications: emaildl1@custdom.com	Ongoing Updates Only 4- or 6-hour updates only: emaildl2@custdom.com CritSit Communications for Regular Incidents	Major Incident Communications emailmirpdl3@custdom.com Redirect to Services Health for Service Incidents

Microsoft recommends customers create their own email DL(s)

*Best practice is for the customer to maintain **DL** membership and provide **DL email** alias for Microsoft to send **notifications** to*

Microsoft confidential. For internal use only

CritSit Communications Example

Initial Email Example

Hello,

Microsoft has received your "Severity A / Critical" Service Request, as your Incident Manager I am your escalation point of contact in business hours, if the case progresses out of business hours I will provide further details upon handover at the end of my day.
The contact information we have for you is as follows (please let us know if there are others):

Contact Information:
Customer name
Phone
Email:

How to contact us:
If the incident status changes or you have additional information to share, please respond to this email.
For any other questions or concerns regarding the status of this incident, please feel free to contact me.

Thank you,
Im name
Microsoft Incident Management Team

This message from Microsoft is an important part of a program, service, or product that you or your company purchased or participate in. Microsoft respects your privacy.
Please read our Privacy Statement.
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Legal Disclaimer: The information contained in this message may be privileged and confidential. It is intended to be read only by the individual or entity to whom it is addressed or by their designee. If the reader of this message is not the intended recipient, you are on notice that any distribution of this message, in any form, is strictly prohibited. If you have received this message in error, please immediately notify the sender and delete or destroy any copy of this message
EU Customers only: The European Commission provides an online dispute resolution platform, which can be accessed here: http://ec.europa.eu/consumers/odr/ More information on this is available here: https://www.microsoft.com/en-us/legal/arbitration/EU-ODR.aspx .

Update Email Example

Hello ,

Below is a summary of the critical incident we are currently working on. You are receiving this update because you have been identified as an important stakeholder. I am the Critical Situation Manager who has been assigned to help manage this incident and will provide you with regular updates until the incident has been resolved or severity has been reduced.

Current Status:
It was requested the collaboration from the Microsoft Product Group (PG) to perform an in-depth analysis of the issue. Meanwhile, the investigation is ongoing to provide the mitigation on the issue.

Next Steps:
Microsoft:
- Monitor the progress of Microsoft Product Group and share updates accordingly

Customer:
- Stand-by for feedback from Microsoft

Next Planned Update: 6 hours from the current update

Issue Summary:

Case #	
Description of Incident	There is an issue with Exchange Online, where the Microsoft Stream service is down.
Creation Date	2/25/2021 12:58:10 PM UTC
Business Impact	All the users are not able to access to the Microsoft Stream service, due to the web side is unavailable, preventing the access to video recordings, upload or download videos. Hence, important data is stored on this service.
Products Impacted	Exchange Online

How to contact us:
Please do not hesitate to email or call if you have any questions or concerns about the issue.

Thank you,
Name
Critical Situation Manager | Critical Situation Management and Escalation Team
Customer & Field Engagement | For Customer Service and Support

Phone numbers by region:

- Korea +82 80 808 1661
- Australia + 61 1 800 006 257
- Europe, Middle East, Africa, + 44 118 909 5447
- Hong Kong + 852 2804 4030
- India + 91 80 6179 6666
- Indonesia + 62 21 515 4649
- New Zealand + 64 800 274 874
- South East Asia + 65 6238 8219
- US & Canada + 1 888 859 7425
- Latin America – Call your local Premier Phone and request to be transferred.

Customer Incident Communication DL

Microsoft | Support

Hello (Contact for Incident),

Thanks for reporting the (impacted service) issue, that is impacting the users in your organization.

The issue you have reported is impacting multiple customers and is a high priority. Our engineering team is already engaged, working towards a resolution.

Regular updates will be published directly to your Service Health Dashboard. Please choose your corresponding product below to view your dashboard for all further updates.

Your Premier Relationship Manager should be aware of this issue. Once this is resolved, your Service Health dashboard will be updated.

Microsoft 365 and **Dynamics 365 Resources** *Including:* • *Microsoft 365 (and Intune)* • *Azure AD* • *Dynamics 365*	To read the latest updates on this incident, check Service health in the Microsoft 365 admin center.* If there are issues accessing the Admin center, check the Microsoft 365 public status page Twitter handle: @MSFT365Status is also updated for broadly impacting Microsoft 365 incidents. If you haven't done so already, we recommend downloading the Office365 Mobile App. It will help you keep track of your Azure resources on the go – enable push notifications for alerts about any future issues impacting your services. *If impact/issue you are experiencing doesn't match the incident reported in Service health, then please reply to this email. Please note that there could be delays in response due to the ongoing service incident.
Azure Resources *Including:* • *Azure services* • *Azure AD* • *DevOps*	To read the latest updates on this incident, check Service Health in the Microsoft Azure portal.* If there are issues accessing the portal, check the Azure status page. While in Azure Service Health, we also recommend that you set up ***service health alerts*** to notify you and your teams automatically during any future service issues, planned maintenance, or health advisories. By setting these up, you will be alerted via your preferred communication channels including email, text message, webhook, and more. Twitter handle: @AzureSupport is also updated for broadly impacting incidents. If you haven't done so already, we recommend downloading the Azure Mobile App. It will help you keep track of your Azure resources on the go – enable push notifications for alerts about any future issues impacting your services. *If the impact/issue you are experiencing doesn't match the incident reported in the Azure portal, then please reply to this email. Please note that there could be delays in response due to the ongoing service incident.

We're sorry for the inconvenience.

Thank you,

Primary Usage for this distribution list is when a customer has created a Support Request indicating a business-critical severity issue.

During issue triage with CritSit manager, *if it is determined that the issue is a Service Incident*, then the CritSit manager will send an email to the Major Customer Communication DL to redirect communications to Service Health in the impacted platform.

Change Management Overview

Microsoft commitment, goals and communication channels

Change Management in the Cloud

Managing Change in the Cloud is Different

- In the cloud service innovation is continuous and needs to be managed differently
- Customers need to understand how services are used and become advocates of productivity within the organization
- In the cloud, managing change is an evergreen program delivering continuous innovation to end users

Microsoft's Change Mission

Enable rapid delivery, improve productivity, and delight customers with new applications and features while minimizing friction and disruption

Change Management Goals

Microsoft strives to provide timely, targeted, and accurate change communication to ensure customers are prepared to manage change.

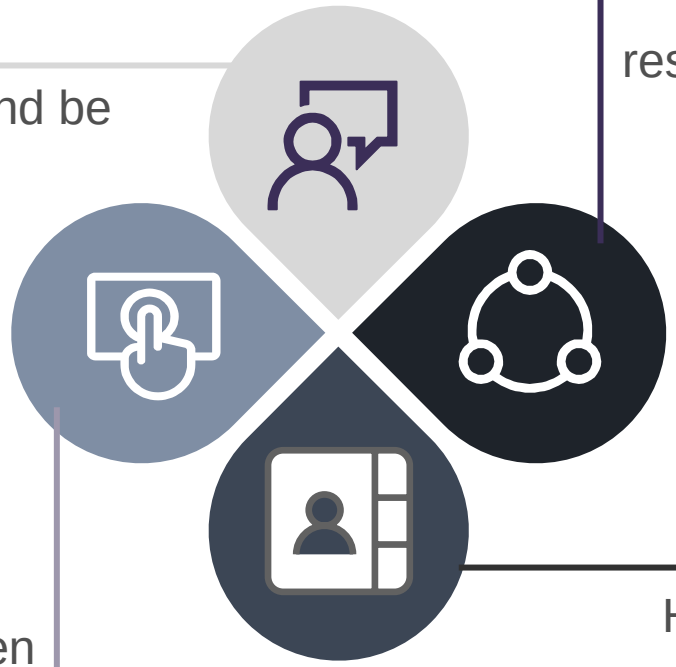
We want to provide a service where customers place their focus on running their organizations and less on managing change.

Purpose

The Azure Change Management Plan is an essential component for Azure customers to plan for and manage change.

Ensure stakeholders are clear about respective roles and responsibilities

Help customers understand change and be prepared to respond effectively



Understand expectations when action is required

Have contact information for all parties engaged

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Change Components, Tools, and Channels

How does Azure communicate at scale?

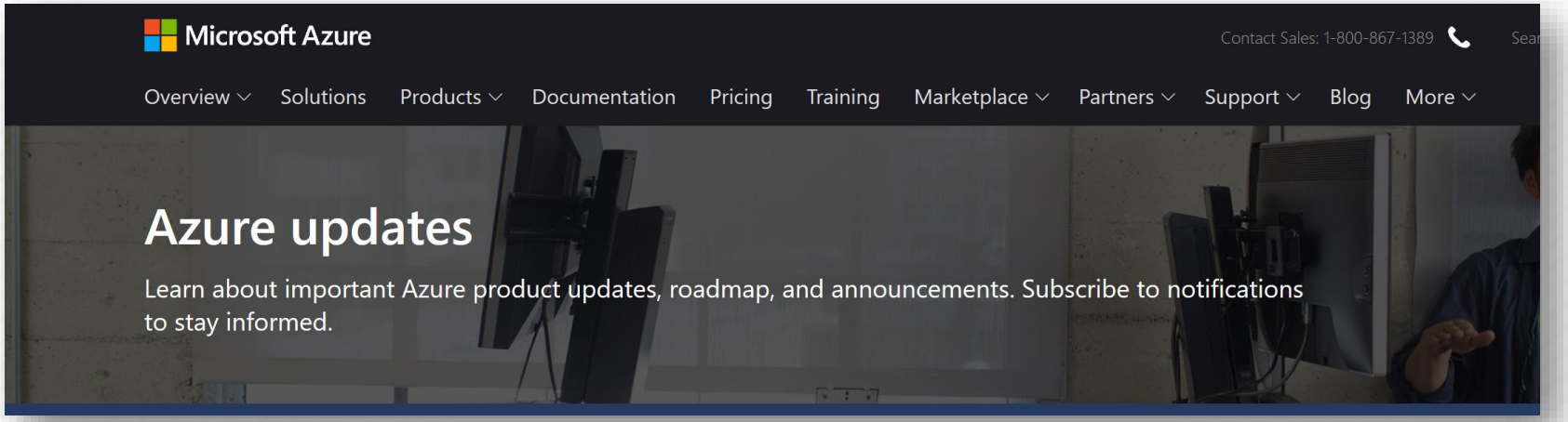
Inform	Advise	Alert
Roadmap		
Azure updates	Azure Advisor	Azure Service Health
Product available by region	Cost Management	Service emails
Blogs and newsletters	Azure Security Center	Azure Monitor
Documentation		

How we listen at scale:

Service telemetry | Support requests | User voice | Research | Events | Community

Azure Updates

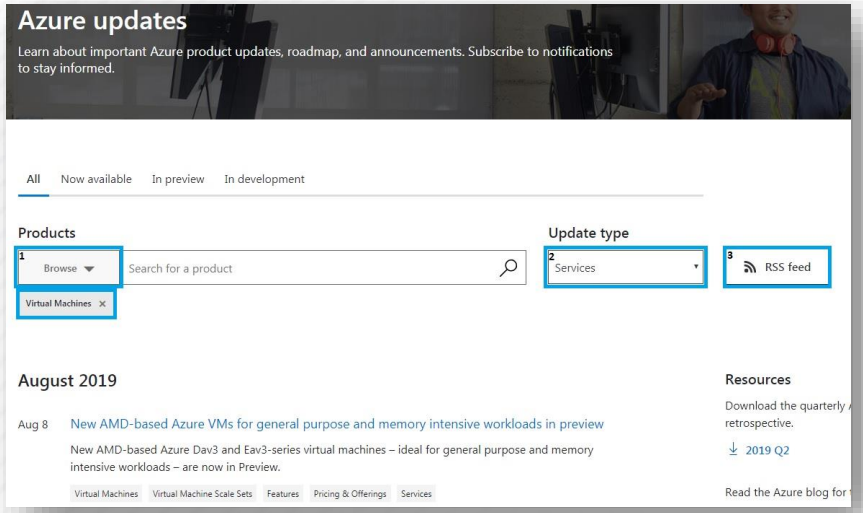
- Now Available
- In Preview
- In Development

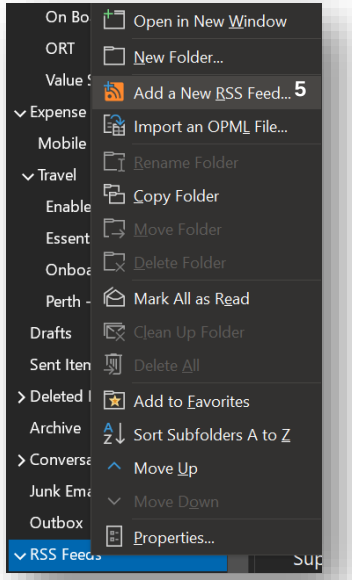


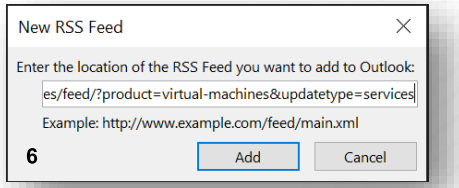
https://azure.microsoft.com/en-us/updates/?query=government

Set up RSS feed (Outlook)

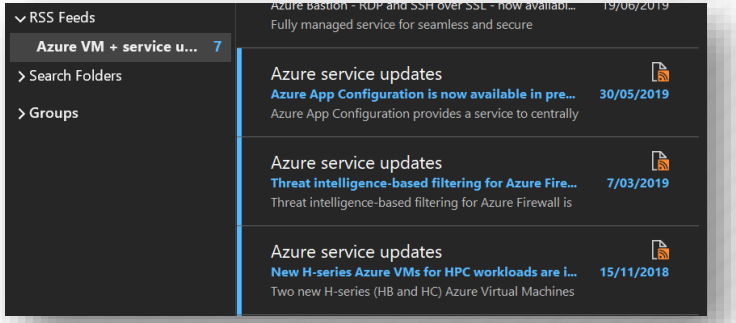
Create an RSS feed based on product & update type to track change notifications from the Azure updates page. Outlook can be utilized to consume the RSS feed.







6. Paste **RSS URL**



1. Select the **Product**
2. Select the **update type**
3. Click on **RSS feed**
4. Copy the **RSS URL**

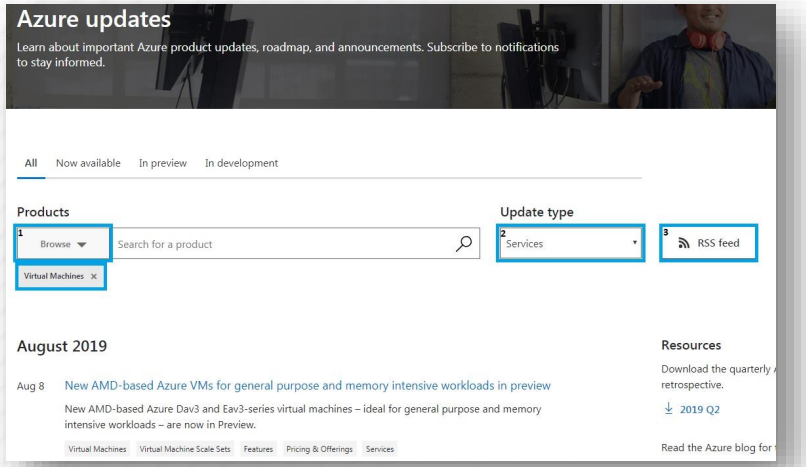
5. Select **Add New RSS Feed**

7. **RSS Feeds Folder** is created to obtain updates

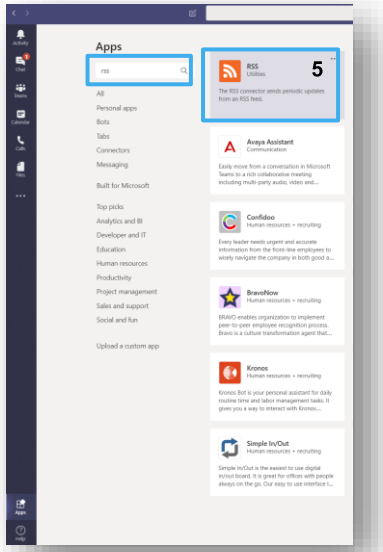
MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Set up RSS feed (Microsoft Teams)

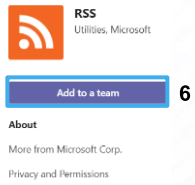
Create an RSS feed in Teams to notify a specific group of SMEs / Application team about changes specific to their Azure Services.



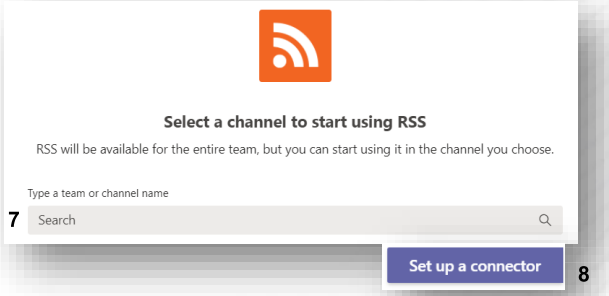
1. Select the **Product**
2. Select the **update type**
3. Click on **RSS feed**
4. Copy the **RSS URL**



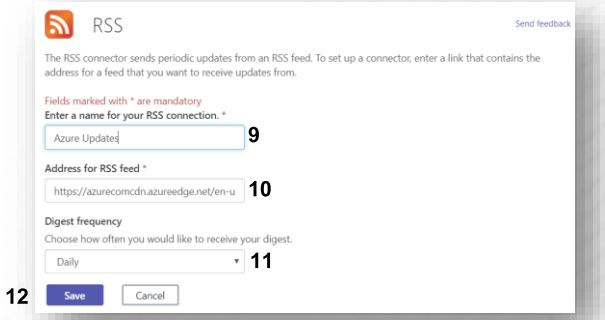
5. Select **RSS**



6. Click **Add to a team**



7. Select a **Teams site** to consume the feed
8. Click **Set up Connector**



9. **Name** the feed
10. Paste **RSS URL**
11. Select **Digest Frequency**
12. Click **save** to complete the Set up

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

How does Azure communicate at scale?

Inform ← → Advise ← → Alert

Azure updates

Product available by region

Blogs and newsletters

Documentation

Azure Advisor

Cost Management

Azure Security Center

Service Health

Azure Service Health

- Service Health
- Planned Maintenance
- Service Advisories

Azure Monitor

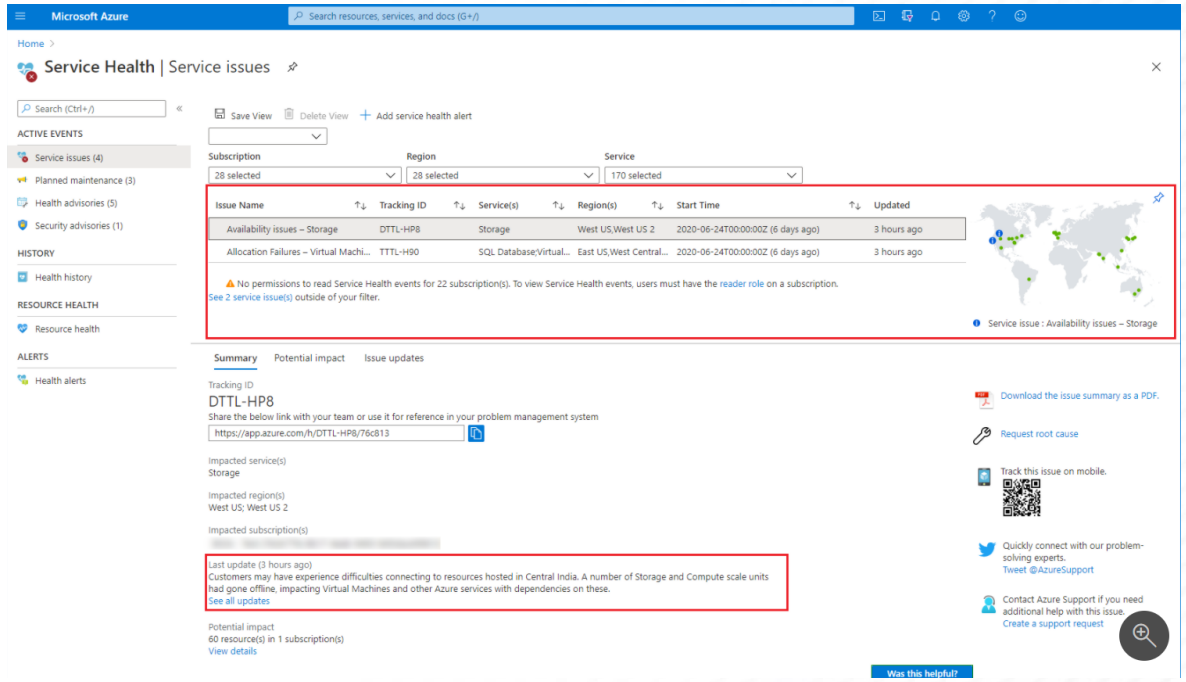
How we listen at scale:

Service telemetry | Support requests | User voice | Research | Events | Community

Maintenance Announcements in the Service Health Dashboard

We’ve focused on highlighting and communicating when Maintenance will be conducted

- **Azure status** - A global view of the health of Azure services
- **Service Health** - A personalized view of the health of your Azure services
  - **Service Issues:** Problems in Azure that affect you right now.
  - **Planned Maintenance:** Planned maintenance that may affect availability.
  - **Health Advisories:** Issues that you need to act to, to avoid disruption
  - **Security advisories** - Security related notifications or violations that may affect the availability of your Azure services.
- **Resource Health** - A deeper view of the health of the individual resources provisioned to you by your Azure services

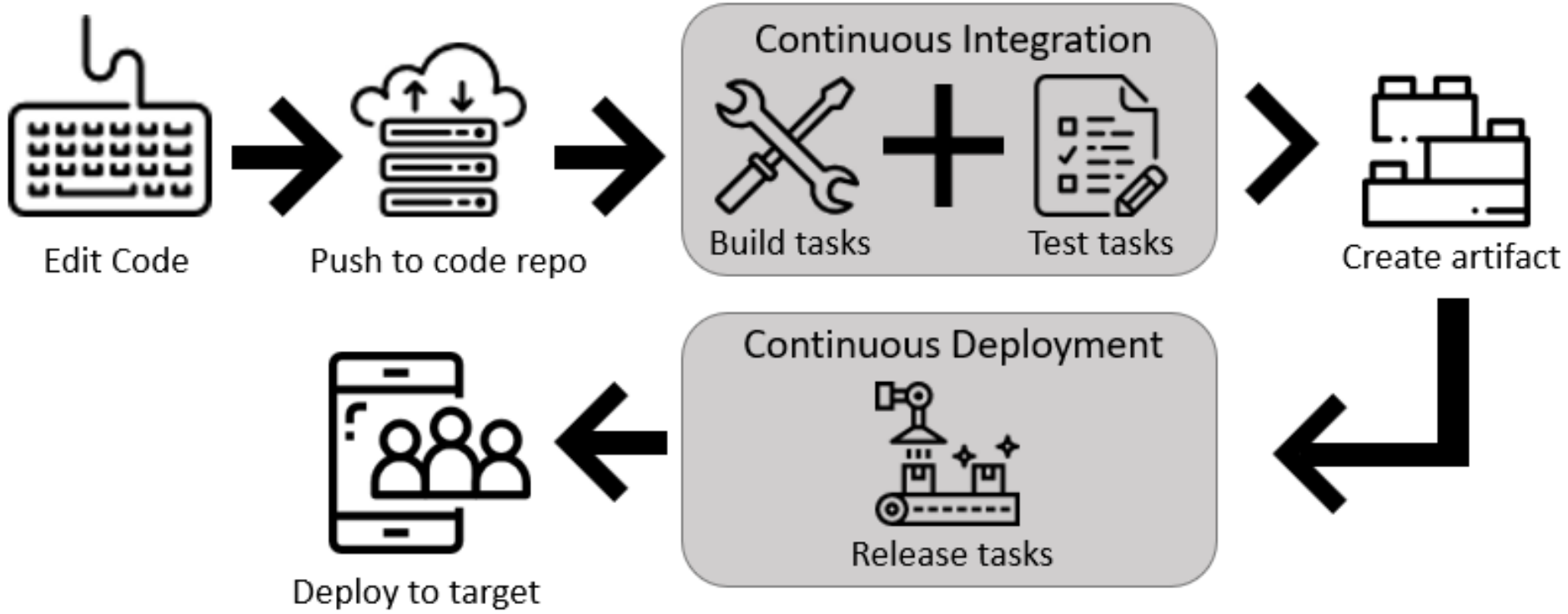


MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

Deployment Pipelines

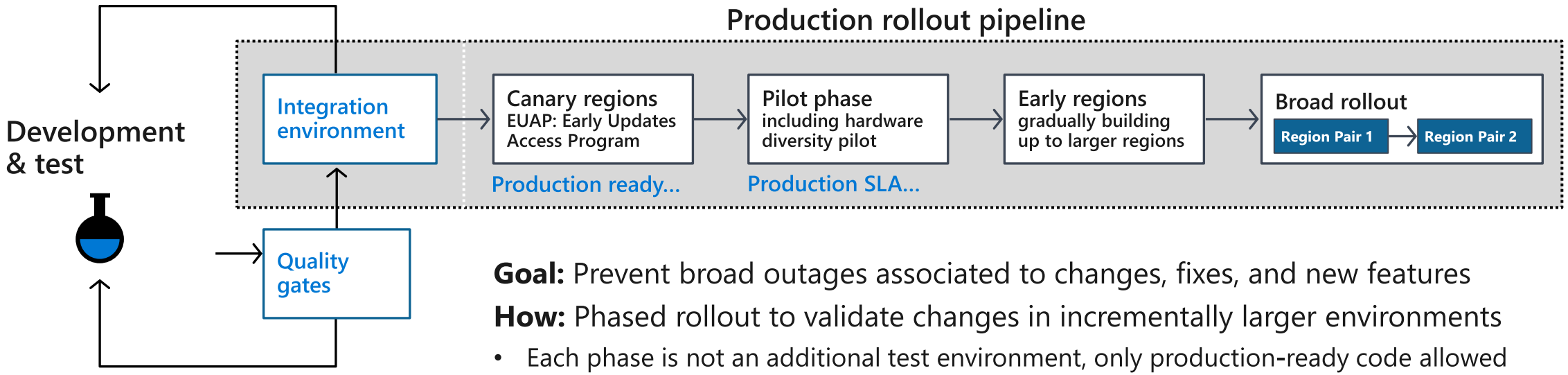
Optimize and Control Change through Pipeline Automation

- Infrastructure as code (IaC)
- Configuration as code (CaC)



Azure Change Automation

Simplified safe deployment practices



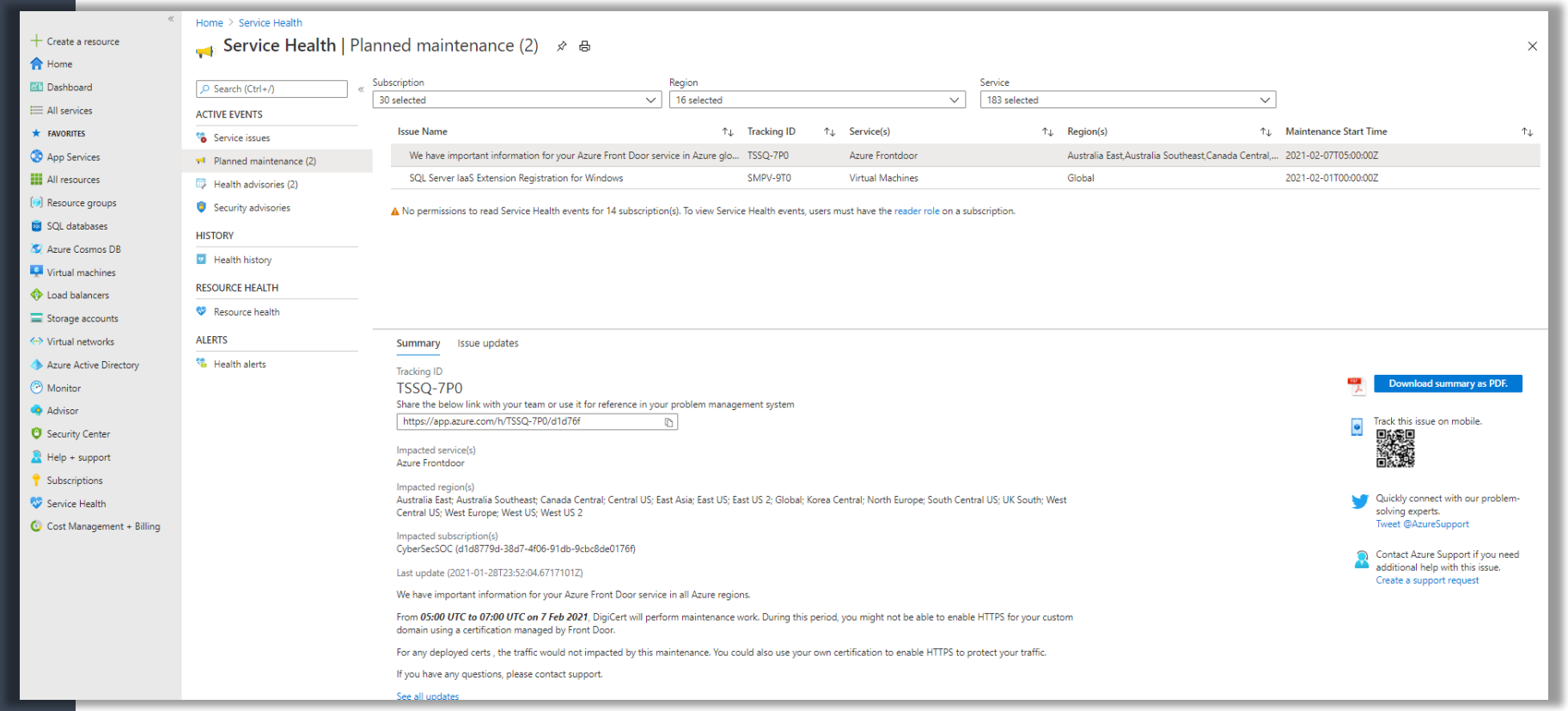
Goal: Prevent broad outages associated to changes, fixes, and new features

How: Phased rollout to validate changes in incrementally larger environments

- Each phase is not an additional test environment, only production-ready code allowed
- Stability and reliability of each stage is comparable to general production environment
- All environments utilize platform health signals to determine the suitable rollout velocity

Increasing cost and impact of failures

Maintenance Announced in the Planned Maintenance Dashboard



Planning

Identifying key contacts for upcoming Azure changes

Change Management for Azure

Before the Change	During the Change	After the Change
Identify a CCOE / Governance Board and validate policies	Consider the changes' impact to your organization and your end users	Provide feedback about an upcoming service change at https://feedback.azure.com or by using feedback button in Azure Portal
Know about the change • Check the Azure Product Roadmap • Check Service Health \ Planned maintenance or Health Advisory • CSAM, Account Team, Peers & More	Stay aware of workflow changes to help deployment teams and increase end user productivity	Review factors that drive successful deployment in your organization and adapt to reduce impact and increase awareness and efficiency
Provide feedback about an upcoming service change at https://feedback.azure.com or by using feedback button in Azure Portal	Ensure the stakeholders and contacts section is complete and provided to your CSAM	Changes are designed to benefit customers. Help your users be aware of changes, understand them, and get the most value out of them

Change Communication Planning

High Level Questions to Answer:

1. Who will identify what changes are coming and when?
2. Who needs to know about the change (recipients)?
3. Who needs to communicate the change details (sender) – multiple recipients and messages may be required (i.e. admins, makers, users all have different requirements to effectively understand and consume changes)?
4. What tasks are required to apply changes through the environments?

Typical Roles Involved

Project Managers
Cloud Architects
IT Process Owners (Incident / Change / Release)
Executive Sponsor
Helpdesk admin
User admin
License admin
Billing admin
Compliance admin
Application admin
Application developers
Authentication admin
System Administrator
System Customizer
Business Administrator
Business Owners
Service Owners
End Users
Application Makers
Analysts

Creating a Cloud Change Management Plan

Step 4.
Help customers understand change and be prepared to respond effectively

Step 1.
Ensure stakeholders are clear about respective roles and responsibilities

Step 3.
Understand expectations when action is required

Step 2.
Have contact information for all parties engaged

Stakeholder Roles and Responsibilities

RACI R=Responsible A=Accountable C=Consulted I=Informed

	Service Owner	Product Owner	Architect	Iaas Compute Admin	PaaS Storage admin	PaaS DB admin	PaaS integration admin	App Dev Lead	Identity AAD admin	App Services Admin	Network admin	Monitor admin	Comm's Lead	Training Lead	Compliance Admin	Security Admin	Incident Manager	Change Manager
Review Azure Roadmap																		
Create customer specific roadmap																		
Review Planned Maintenance Blade																		
Identify Changes with Impact																		
Perform compliance reviews																		
Perform security reviews																		
Test and validate new updates																		
Prepare user notification																		
Prepare user documentation																		
Prepare user training																		
Prepare admin notification																		
Prepare admin documentation																		
Prepare admin training																		
Prepare internal help-desk																		
Create RFCs / Submit to CAB*																		
Release updates to end users (feature controls)																		

*When Azure Changes create related changes in the environment (typically changes requiring admin action)

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

Roles and Responsibilities Example

RACI R=Responsible A=Accountable C=Consulted I=Informed

	Service Owner	Product Owner	Architect	Iaas Compute Admin	PaaS Storage admin	PaaS DB admin	PaaS integration admin	App Dev Lead	Identity AAD admin	App Services Admin	Network admin	Monitor admin	Comm's Lead	Training Lead	Compliance Admin	Security Admin	Incident Manager	Change Manager
Review Azure Roadmap	A	I	R	R	R	R	R		R	R	I	R	I	I	I	R	I	I
Create customer specific roadmap	A	R	C	C	C	C	C	C	C	C	C	C				C		C
Review Planned Maintenance Blade	A	C	R	R	R	R	R	R	R	R	R	R			I	C		I
Identify Changes with Impact	A	C	R	R	R	R	R	R	R	R	R	R		C	I	C		I
Perform compliance reviews	A	C	C	C	C	C	C	C	C	C	C	C			R	C		
Perform security reviews	A	C	C	C	C	C	C	C	C	C	C	C			C	R		
Test and validate new updates	A	I	C	R	R	R	R	R	R	R	I	R	I	I	C	R	I	I
Prepare user notification	A	R	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Prepare user documentation	A	C	C	C	C	C	C	C	C	C	C	C	R	R	C	C	C	C
Prepare user training	A	C	C	C	C	C	C	C	C	C	C	C	R	R	C	C	C	C
Prepare admin notification	A	I	C	R	R	R	R	R	R	R	I	R			R	R		
Prepare admin documentation	A	I	C	R	R	R	R	R	R	R	I	R			R	R		
Prepare admin training	A	C	C	C	C	C	C	C	C	C	C	I	C	R	C	C	C	C
Prepare internal help-desk	A	C	C	C	C	C	C	C	C	C	C	I	C	R	C	C	C	C
Create RFCs / Submit to CAB*	A	C	R	R	R	R	R	R	R	R	R	R			I	C		I
Release updates to end users (feature controls)	A	C	C	C	C	C	C	R	C	C	C	C	C	C	C	C	C	C

*When Azure Changes create related changes in the environment (typically changes requiring admin action)

MS FEDERAL CLOUD & CUSTOMER EXPERIENCE TEAM

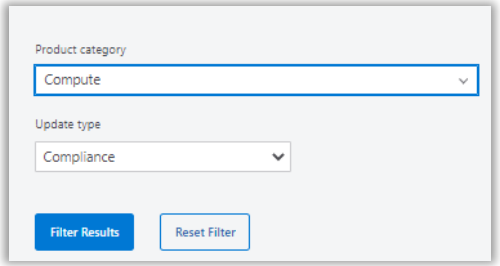
Stakeholder Contact Information

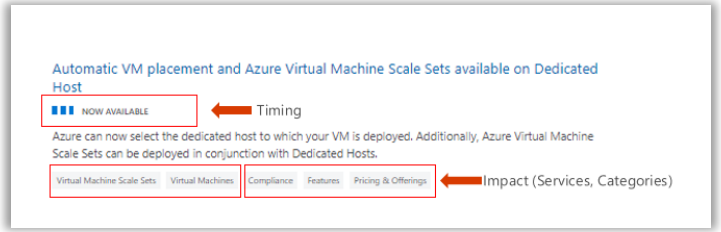
Role	Name	Email	Phone	Office / Location
Service Owner				
Product Owner				
Architect				
Compute Platform admin				
Database Platform admin				
Storage Platform admin				
<service> Platform admin				
Identity / AAD admin				
Groups admin				
User admin				
Service Support admin				
Helpdesk admin				
Network admin				
Communications Lead				
Training Lead				
Compliance Admin				
Security Admin				
Change / Release Manager				
Governance Lead				
Business App Owner				
Business App Owner				

Set Expectations for When Action is Required

- Prioritize Capabilities
- Publish / update a Roadmap tailored for the enterprise
- Identify who is impacted and how they are impacted
- Perform Adoption Planning
- Identify the types of action required
  - Notifications
  - Training
  - Environment changes
  - Testing and validation
  - etc…

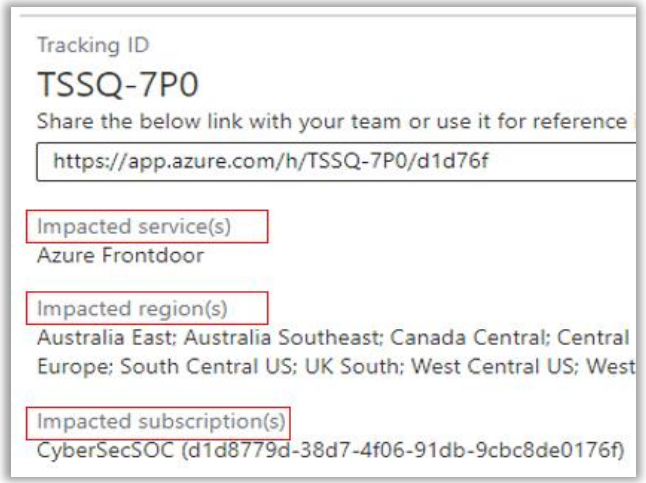
Review Azure Updates





Review Service Health

Planned Maintenance | Health Advisories | Security Advisories



Prepare Customers for Change

Organizational Change Readiness

- Communications Plan - Create awareness and set expectations
  - Target stakeholders: identify by role and type of impact

- Training Plan – Right sized approach to ensure users and administrators can consume changes
  - “Battle Cards”
  - Work instructions
  - Formal Training

Build, Adoption and Change Plan

Make sure to plan on the adoption of new features available in a release wave to ensure the most value is delivered to the business

Envision

Identify and prioritize scenarios while learning about available resources as you plan for rollout. This stage is critical to your journey as you're setting business goals to measure success.

Assemble Your Team
Define Business Strategy
Determine Readiness

Onboard

Work with your key stakeholders to build and launch your adoption plan. Prepare your environment and test your adoption approach with Early Adopters. Use feedback to adjust before scaling to the business.

Build Your Adoption Plan
Launch to Early Adopters
Adjust Your Plan

Drive Value

Full-scale deployment and business success depend on usage and satisfaction. This requires planning through the Envision and Onboard phases plus ongoing operational excellence.

Monitor End User Adoption
Measure and Report Usage
Encourage Ongoing Engagement

Resources

- **Azure Service Health** online documentation (https://azure.microsoft.com/en-us/features/service-health/)
- Service Health at the public **Azure Status page**. (https://status.azure.com/en-us/status)
- **Azure Updates for Government: https://azure.microsoft.com/en-us/updates/?query=government**
- **Optimize your environment with the System Center Operations Manager Health Check (Preview) - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/scom-assessment**
- **Azure Monitor Overview: https://docs.microsoft.com/en-gb/azure/azure-monitor/overview**
- **Azure Monitor data platform: https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/data-platform**
- **Handling planned maintenance notifications: https://docs.microsoft.com/en-us/azure/virtual-machines/maintenance-notifications?toc=/azure/virtual-machines/windows/toc.json&bc=/azure/virtual-machines/windows/breadcrumb/toc.json**

Resources (cont.)

- **What is Azure Monitor? (5:00 3/13/2020):** https://www.youtube.com/watch?v=eSutaPE80PM
- **Differences between Azure Service Health, Resource Health, and Status (2:04 4/1/2019:** https://www.youtube.com/watch?v=xKMfSSGk9gU
- **Is Azure up? Outages, resilience, and Azure Service Health alerts video. (7:14 9/18/2019):** https://www.youtube.com/watch?v=7bDR7xjrN2w
- https://docs.microsoft.com/en-us/azure/devops/pipelines/get-started/what-is-azure-pipelines?view=azure-devops#deployment-targets
- **Microsoft Ignite Demonstration of CritSit Communication Scenarios (46:33 10/25/2018):** https://www.youtube.com/watch?v=8HW87XmlPOE

- **Twitter Support Notifications:**
  - https://twitter.com/MSFT365Status @MSFT365Status [Useful for Azure Active Directory updates]
  - https://twitter.com/AzureSupport @AzureSupport

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

- Azure Monitor
- Azure Status
  - Service Health
  - Resource Health
  - Service Incident Overview
  - CritSit Overview
  - Major Incident Preparedness
- Azure Alerts
- Change Management

MS FEDERAL
CLOUD & CUSTOMER
EXPERIENCE TEAM

THANK YOU!