TROUBLESHOOTING GUIDE FOR AZURE SERVICES

DHAIRYA PAHWA
REDBACK OPERATIONS

Table of Contents

INTRODUCTION

PURPOSE OF THE GUIDE

This section provides a concise explanation of why the troubleshooting guide exists. It outlines its primary goal, which is to assist users in resolving issues they encounter while using Azure services. The overview may highlight the guide's focus on providing step-by-step instructions, tips, and best practices to efficiently troubleshoot common problems users may face in their Azure deployments.

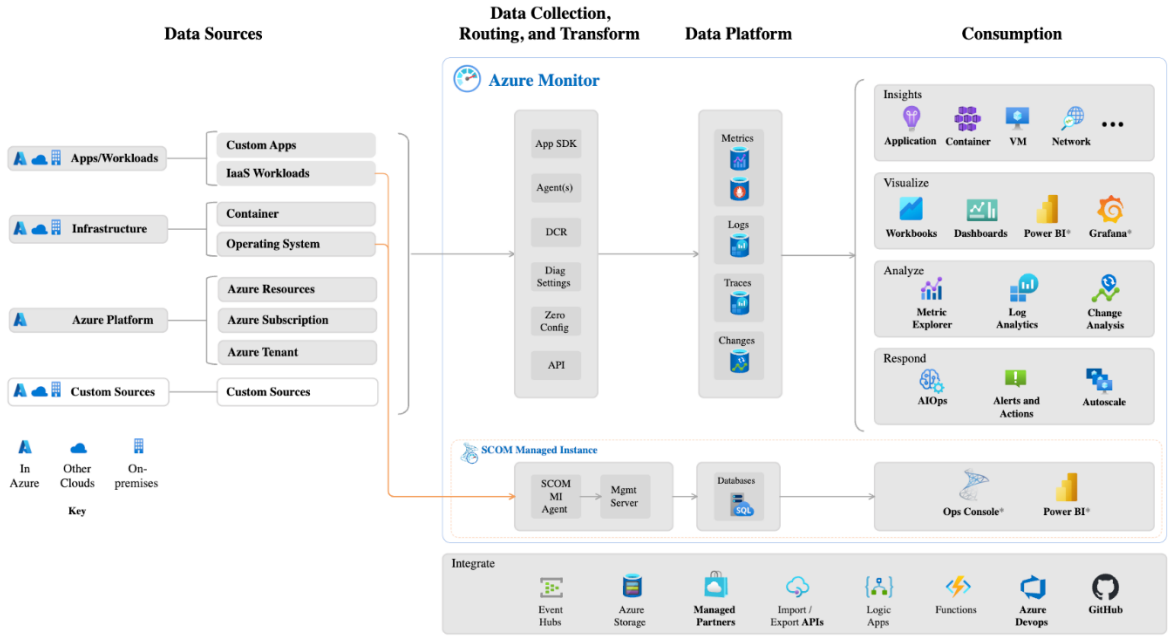
IMPORTANCE OF TROUBLESHOOTING FOR AZURE SERVICES

Here, the guide emphasizes the significance of troubleshooting in the context of Azure services. It underscores that as users leverage Azure's vast array of cloud solutions, they may encounter technical challenges or unexpected behaviour. Effective troubleshooting ensures that these issues are swiftly identified and resolved, minimizing downtime, optimizing performance, and enhancing user experience. The importance of troubleshooting extends beyond mere problem-solving; it fosters a deeper understanding of Azure services and builds expertise among users.

DISCLAIMER ABOUT THE DYNAMIC NATURE OF CLOUD SERVICES AND THE NEED FOR UPDATED INFORMATION

This disclaimer acknowledges the ever-evolving nature of cloud services, particularly Azure. It underscores that the information provided in the troubleshooting guide is based on current knowledge and best practices at the time of writing. However, due to frequent updates, feature enhancements, and service changes by Azure, some information within the guide may become outdated over time. Users are encouraged to regularly consult official Azure documentation, support resources, and community forums for the most up-to-date information and guidance. This disclaimer promotes a proactive approach to troubleshooting and reinforces the importance of staying informed about changes in Azure services.

SECTION 1: COMMON ISSUES



1.1 *VIRTUAL MACHINES (VMs)*

We'll guide you through retrieving troubleshooting information from Microsoft's website, focusing on two common issues:

RDP Setup Issue: Users often face challenges setting up RDP connections to Azure VMs due to configuration errors and network issues. Troubleshooting involves verifying settings, firewall rules, RDP enablement, and user credentials.

VM Not Accessible Issue: Inaccessibility of Azure VMs may stem from network configuration, authentication, or resource constraints. Troubleshooting entails checking NSG rules, verifying VM credentials, and monitoring resource utilization. Accessing Microsoft's documentation offers detailed guidance for resolving these issues efficiently.

ISSUE 1- RDP SETUP ISSUE

Enter the diagnose and solve experience, you can see a bunch of common problems tiles, so those are common problems that you identify together with Azure compute product teams, Microsoft support teams, and dev teams. So, that includes a bunch of different kinds of virtual machine issues, such as deployment, connectivity, and performance management, all kinds of different problems.

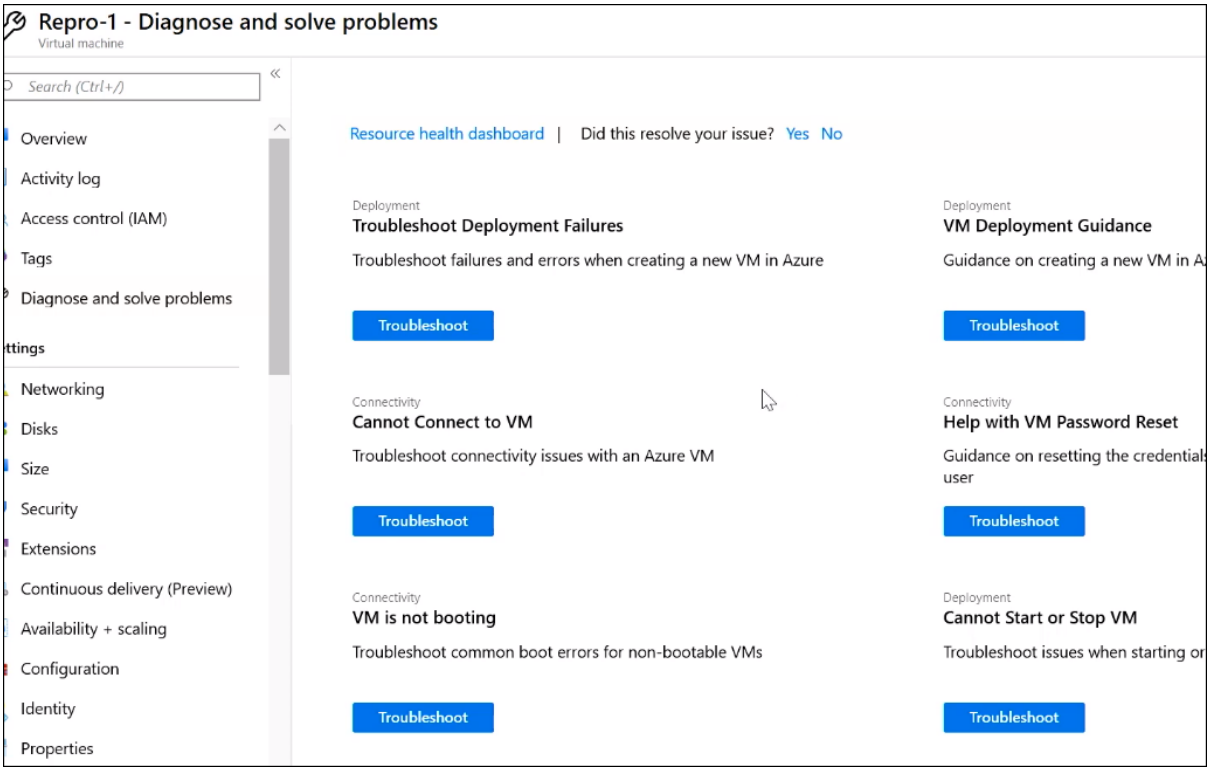
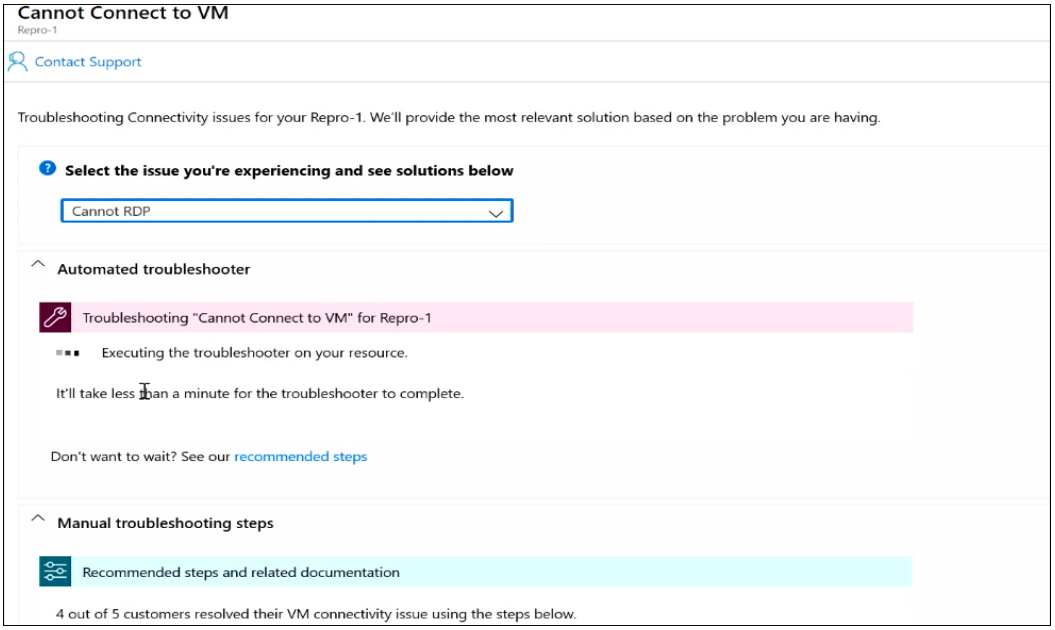
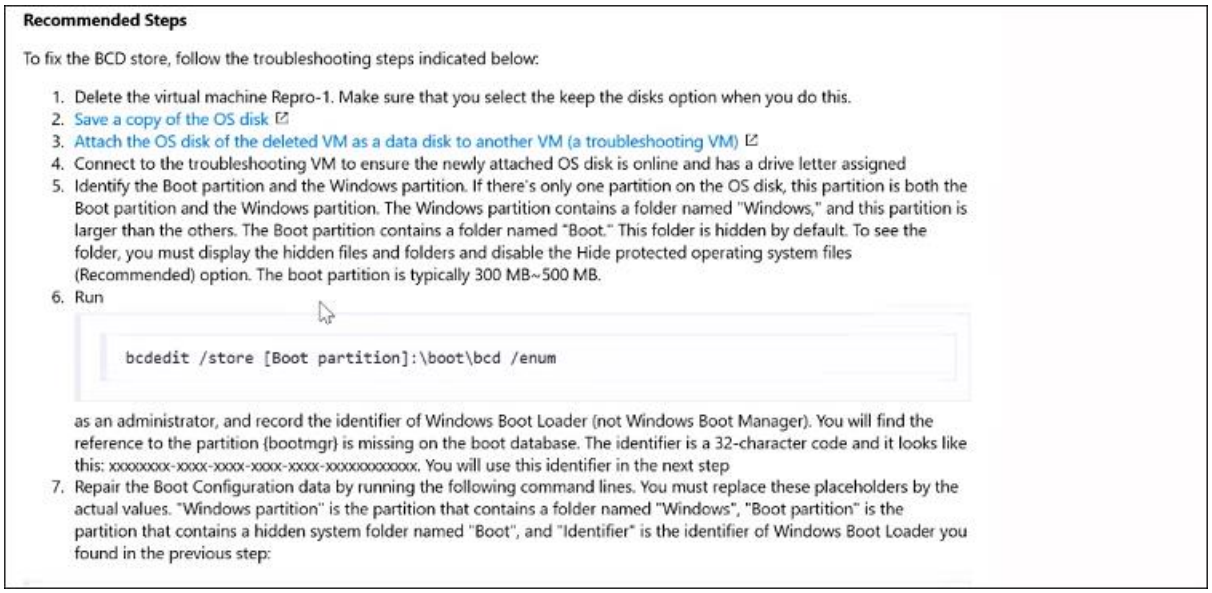


Figure 1 Diagnose and solve problems window.

So, basically, another important thing is that the content that is displayed there are some of the most common issues based on data from customers, engineering, content, etc. When you click on can't connect to VM because you cannot via RDP and select cannot RDP it automatically gives you the troubleshooter and it takes less than a minute to run on your virtual machine. And it tells you more information about possible reasons that you might not be able to connect your VM, for instance, or you might have your firewall selected correctly. You might not have your network security rules set correctly.



It shows you more information here and it also gives you recommended steps down below that you can follow step by step to troubleshoot your VM issues within clicks.



Recommended Steps

To fix the BCD store, follow the troubleshooting steps indicated below:

1. Delete the virtual machine Repro-1. Make sure that you select the keep the disks option when you do this.
2. Save a copy of the OS disk
3. Attach the OS disk of the deleted VM as a data disk to another VM (a troubleshooting VM)
4. Connect to the troubleshooting VM to ensure the newly attached OS disk is online and has a drive letter assigned
5. Identify the Boot partition and the Windows partition. If there's only one partition on the OS disk, this partition is both the Boot partition and the Windows partition. The Windows partition contains a folder named "Windows," and this partition is larger than the others. The Boot partition contains a folder named "Boot." This folder is hidden by default. To see the folder, you must display the hidden files and folders and disable the Hide protected operating system files (Recommended) option. The boot partition is typically 300 MB~500 MB.
6. Run

```
bcdedit /store [Boot partition]:\boot\bcd /enum
```

as an administrator, and record the identifier of Windows Boot Loader (not Windows Boot Manager). You will find the reference to the partition {bootmgr} is missing on the boot database. The identifier is a 32-character code and it looks like this: xxxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. You will use this identifier in the next step

7. Repair the Boot Configuration data by running the following command lines. You must replace these placeholders by the actual values. "Windows partition" is the partition that contains a folder named "Windows", "Boot partition" is the partition that contains a hidden system folder named "Boot", and "Identifier" is the identifier of Windows Boot Loader you found in the previous step:

You can follow those recommendations step by step, and if you don't want to wait for that automatic troubleshooter to run, an alternative is to use Azure's manual troubleshooting steps. They have a list of documentation that they update regularly that shows you more information on how you can troubleshoot your RDP issues.

Filter by title

disconnects frequently

Troubleshoot a general error

Troubleshoot authentication errors

Troubleshoot Azure VM RDP connection issues by Event ID

Troubleshoot RDP error in VM because of static IP

Troubleshoot RDP error in VM because the NIC is disabled

Troubleshoot RDP error caused by Safe Mode

Disable the guest OS Firewall in Azure VM

Enable or disable a firewall rule

Detailed troubleshooting steps for remote desktop connection issues to Windows VMs in Azure

10/30/2018 • 8 minutes to read •

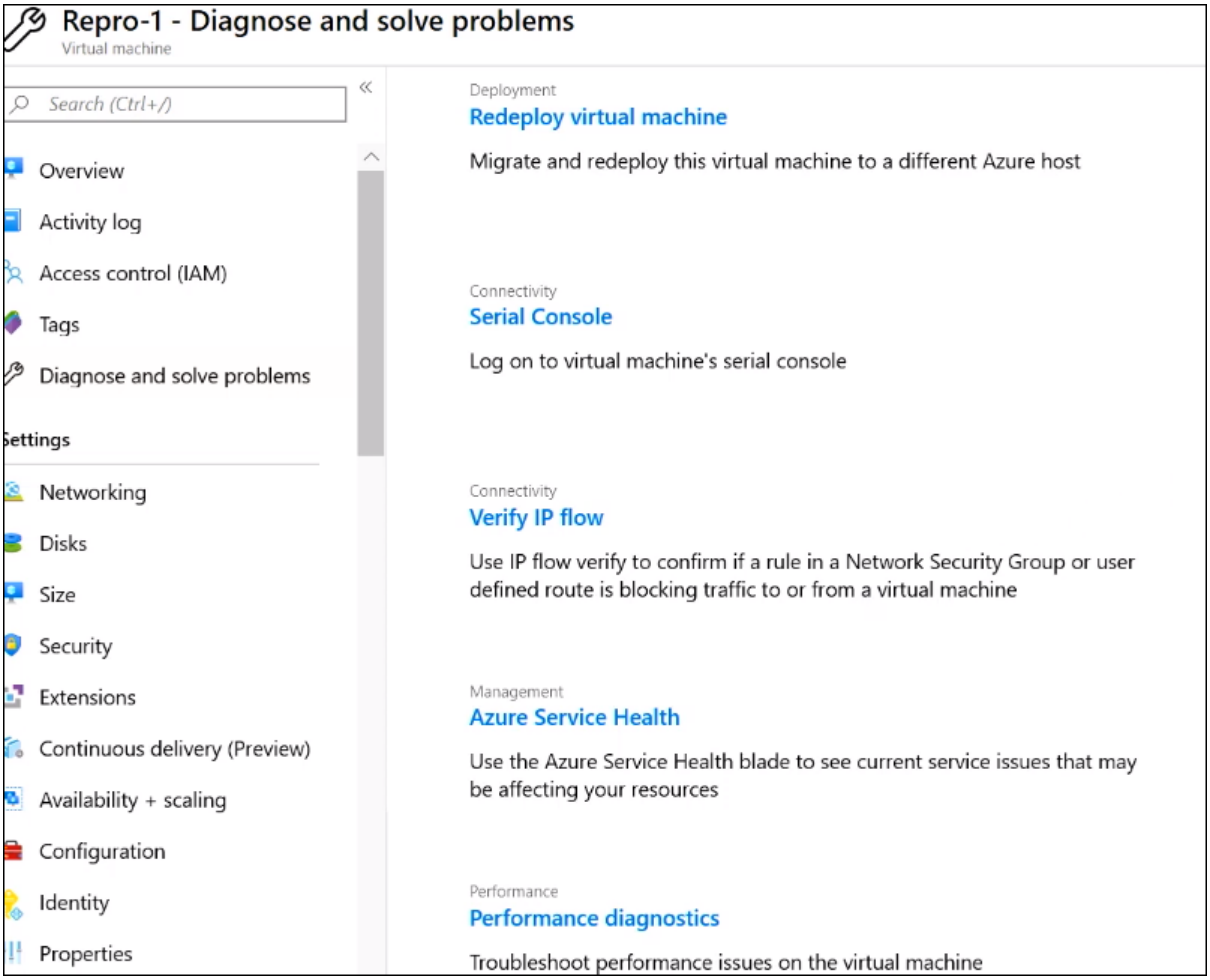
This article provides detailed troubleshooting steps to diagnose and fix complex Remote Desktop errors for Windows-based Azure virtual machines.

Important

To eliminate the more common Remote Desktop errors, make sure to read the basic troubleshooting article for Remote Desktop before proceeding.

You may encounter a Remote Desktop error message that does not resemble any of the specific error messages covered in the basic Remote Desktop troubleshooting guide. Follow

Now, if you want to solve the problems, they can be solved in Azure's diagnose and solve problems section. So, go back to the home page. And you can go from, the troubleshooting tools. On there, you will have a list of tools that Azure also updates regularly based on their dev engineering work.



You can always follow those steps to troubleshoot your connectivity. You have two paths that you can go. One is that you can use the diagnostic tool that is going to tell you what is going on and gives a set of steps. But if you don't want to wait, you want to do that on your own, you offer Azure all the links to the relevant stuff that you can go and learn yourself.

ISSUE 2) VM NOT ACCESSIBLE ISSUE

When your Virtual Machine (VM) becomes inaccessible, it can disrupt your workflow and hinder your operations. This issue could arise due to various reasons, including:

Possible Causes:

1. **Network Configuration Issues:** Incorrect network settings can prevent communication with the VM, leading to inaccessibility.
2. **Authentication Problems:** Incorrect or outdated credentials can hinder access to the VM, especially when using remote access protocols like RDP (Remote Desktop Protocol) or SSH (Secure Shell).
3. **Resource Constraints:** If the VM is under heavy load or has exhausted its allocated resources, it may become unresponsive or inaccessible.

Troubleshooting Steps:

To diagnose and resolve the issue of an inaccessible VM, follow these steps:

1. **Check Network Security Group Rules:**
    - Navigate to the Azure portal and locate the Network Security Group (NSG) associated with your VM.
    - Review the inbound and outbound security rules to ensure that they allow necessary traffic to reach the VM.
    - Adjust the NSG rules if necessary, ensuring that they align with your network requirements.
2. **Verify VM Credentials:**
    - Double-check the credentials (username and password for Windows VMs, SSH key for Linux VMs) used to authenticate and access the VM.
    - Ensure that the credentials are correct and up to date.
    - If necessary, reset the credentials or update them in the remote access client.
3. **Monitor Resource Utilization:**
    - Use Azure monitoring tools or third-party monitoring solutions to analyse the resource utilization of the VM.
    - Check CPU, memory, disk, and network usage to identify any resource bottlenecks.
    - If resource constraints are detected, consider scaling up the VM size or optimizing resource usage within the VM.

Microsoft Guide :- https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/troubleshoot-rdp-connection

1.2 AZURE APP SERVICES

- **Issue: Application Deployment Failure**
    - Users may encounter application deployment failures within Azure App Service, disrupting the deployment process.
- **Possible Causes:**
    - Configuration Errors: Misconfigured settings in the application or deployment configuration can lead to deployment failures.
    - Insufficient Permissions: Lack of adequate permissions for the user or service principal attempting the deployment can result in failures.
    - Deployment Package Issues: Corrupted or incompatible deployment packages can cause deployment failures.
- **Troubleshooting Steps:**
    - Review Application Settings: Verify that all application settings, including connection strings and environment configurations, are accurately configured.

- Check Deployment Logs: Analyze deployment logs to identify any errors or warnings that may provide insight into the cause of the failure.
- Verify Deployment Credentials: Ensure that the credentials used for deploying the application are correct and have the necessary permissions to perform the deployment.

1.1 AZURE STORAGE

Azure Storage

- **Issue: Unable to Access Storage Account**
  - Users may encounter difficulties accessing their Azure Storage account, impeding data operations and access to stored resources.
- **Possible Causes:**
  - Incorrect Connection String: Errors in the connection string configuration can prevent successful connections to the storage account.
  - Permission Issues: Insufficient or incorrect permissions assigned to the user or application accessing the storage account may restrict access.
  - Service Outage: Temporary disruptions or outages in the Azure Storage service can render the storage account inaccessible.
- **Troubleshooting Steps:**
  - Check Connection String: Validate the connection string configuration to ensure accuracy and compatibility with the storage account.
  - Review Storage Account Permissions: Verify that the user or application attempting to access the storage account has the appropriate permissions configured.
  - Check Azure Status Dashboard: Refer to the Azure Status Dashboard to check for any ongoing service disruptions or outages affecting the Azure Storage service.

Section 2: Advanced Troubleshooting

- Advanced troubleshooting techniques may be necessary for complex or persistent issues with Azure Storage access. These techniques could include:
  - Analysing network traffic to identify potential connectivity issues.
  - Utilizing diagnostic tools provided by Azure to diagnose and resolve access problems.
  - Engaging Azure support for assistance in resolving intricate or persistent issues.

SECTION 2: ADVANCED TROUBLESHOOTING

2.1 AZURE NETWORK

- **Issue: High Latency in Virtual Network**
  - Users may experience high latency within their Azure virtual network, impacting the performance of network-dependent applications and services.
- **Possible Causes:**
  - Suboptimal Routing: Inefficient routing configurations may lead to delays in data transmission between network components.
  - Network Congestion: Heavy network traffic or insufficient bandwidth allocation can result in congestion, causing latency issues.
  - Misconfigured Network Settings: Incorrect configurations of network components, such as subnets, gateways, or routing tables, can contribute to latency problems.
- **Troubleshooting Steps:**
  - Diagnose Network Routes: Use network diagnostic tools to analyse the routing paths within the virtual network and identify any suboptimal routes causing latency.
  - Monitor Network Traffic: Utilize network monitoring tools to track network traffic patterns and identify potential congestion points or bandwidth bottlenecks.
  - Review Network Security Settings: Ensure that network security configurations, such as network security groups (NSGs) and firewalls, are correctly configured and not causing latency due to excessive filtering or blocking of traffic.

2.2 AZURE ACTIVE DIRECTORY

- **Issue: Authentication Failures**
  - Users may encounter authentication failures when attempting to access resources managed by Azure Active Directory (AAD), disrupting user access to applications and services.
- **Possible Causes:**
  - Invalid Credentials: Users may be providing incorrect or outdated credentials during the authentication process.
  - AAD Configuration Errors: Misconfigurations in Azure Active Directory settings, such as incorrect authentication methods or policies, can lead to authentication failures.

- Directory Synchronization Issues: Problems with directory synchronization between on-premises Active Directory and Azure Active Directory can result in authentication failures for synchronized users.

- **Troubleshooting Steps:**
  - Verify User Credentials: Double-check the credentials provided by users to ensure they are accurate and up to date.
  - Check AAD Configuration: Review Azure Active Directory configuration settings, including authentication methods, user attributes, and conditional access policies, to identify and correct any misconfigurations.

SECTION 3: RESOURCES AND SUPPORT

- **Official Azure Documentation:**
  - Access comprehensive documentation provided by Microsoft covering various Azure services, including troubleshooting guides, tutorials, and best practices. Visit Azure Documentation.
- **Support Channels:**
  - Utilize official support channels offered by Microsoft for Azure services, including:
    - Forums: Engage with the Azure community and Microsoft experts to seek help, share knowledge, and collaborate on problem-solving. Visit Azure Forums.
    - Support Tickets: Submit support tickets directly to Microsoft for personalized assistance with Azure-related issues. Visit Azure Support.
- **Additional Troubleshooting Resources:**
  - Explore additional troubleshooting resources provided by Microsoft and the Azure community, including:
    - Blogs: Stay updated with the latest Azure updates, tips, and troubleshooting techniques from Microsoft engineers and Azure MVPs. Visit the Azure Blog.
    - Community Forums: Participate in community-driven forums and discussions to exchange ideas, seek advice, and learn from peers' experiences. Visit Azure Community Forums.

CONCLUSION

Effective troubleshooting is paramount for maintaining the reliability and performance of Azure services. By promptly identifying and resolving issues, users can minimize downtime, optimize resource utilization, and ensure a seamless experience for their applications and workloads.

It is essential to stay updated with the latest Azure service status and documentation. Regularly monitoring service status updates and consulting official documentation helps users stay informed about any changes, updates, or known issues affecting Azure services. This proactive approach enables users to anticipate potential challenges, implement best practices, and leverage new features effectively.

By prioritizing effective troubleshooting and staying informed with Azure service status and documentation, users can enhance their productivity, maximize the value of Azure investments, and ensure a smooth and reliable operation of their cloud infrastructure.