



happiest minds
The Mindful IT Company
Born Digital . Born Agile



Microsoft Azure Arc **for Servers to Modernize** **IT (Information Technology)** **Infrastructure**

Over the last few years, the public cloud has evolved and matured to become the foundation of the modern IT infrastructure. Our industry started transitioning from running solutions in on-premises data centers to the **cloud** to make things more scalable and flexible. Unfortunately, not all the enterprises were able to make this transition. There have been many hurdles to overcome the problems, such as data regulation, latency, **security**, etc. None of them were successful as they had their underlying issues. To solve this problem, Microsoft brought in a governance and management model called Azure Arc, which was announced at Ignite of 2019.

This document guides you through an overview of Azure Arc for servers-as-a-service (SaaS) available on Microsoft Azure, which provides a management and governance solution on Azure Cloud for on-prem servers. The targeted audience of this document is those who are on their way to modernizing and looking to enhance their IT **infrastructure**.

Introduction to Azure Arc

Azure Arc simplifies management and governance by delivering a reliable and consistent multi-cloud and on-premises management platform. Azure Arc enables you to manage physical and virtual machines running on Windows or Linux outside of Azure. So, leveraging Azure arc delivers the following advantages:



1. Customers can manage their public cloud resources within and outside of Microsoft Azure through the same centralized, cloud-native management interface.

2. Customers can use Azure Security Center compliance capabilities and security across all cloud services — within Azure and external — registered with Azure Arc. Patching, policies, tags, and more can be automatically pushed out to all your virtual machines (VMs).

3. Customers can use their advanced monitoring and Azure Monitor data for all cloud-based resources registered with Azure Arc, whether they are Azure or not.

4. Customers who leverage Azure Resource Manager (ARM) templates can get benefits like Role-Based Access Control (RBAC), policies for Virtual Machines outside/inside of Azure, and universal resource management through the Azure Policy.

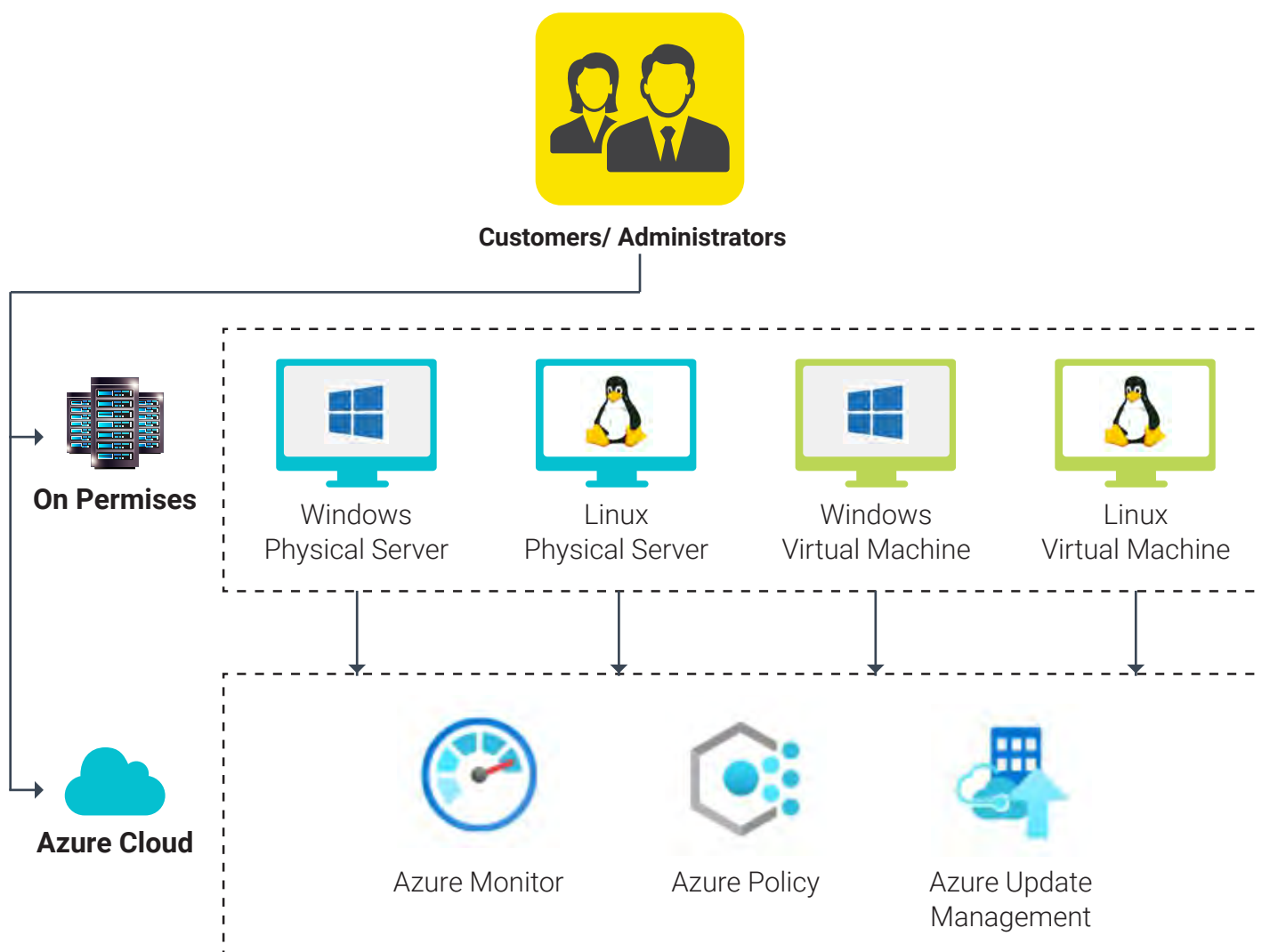
5. Azure Arc is available free of cost.

From the Azure arc management plane, we can manage our entire environment with a single plane of glass by projecting our existing non-azure, on-premises, or other-cloud resources into the Azure Resource Manager.

Azure Arc Resource Manager

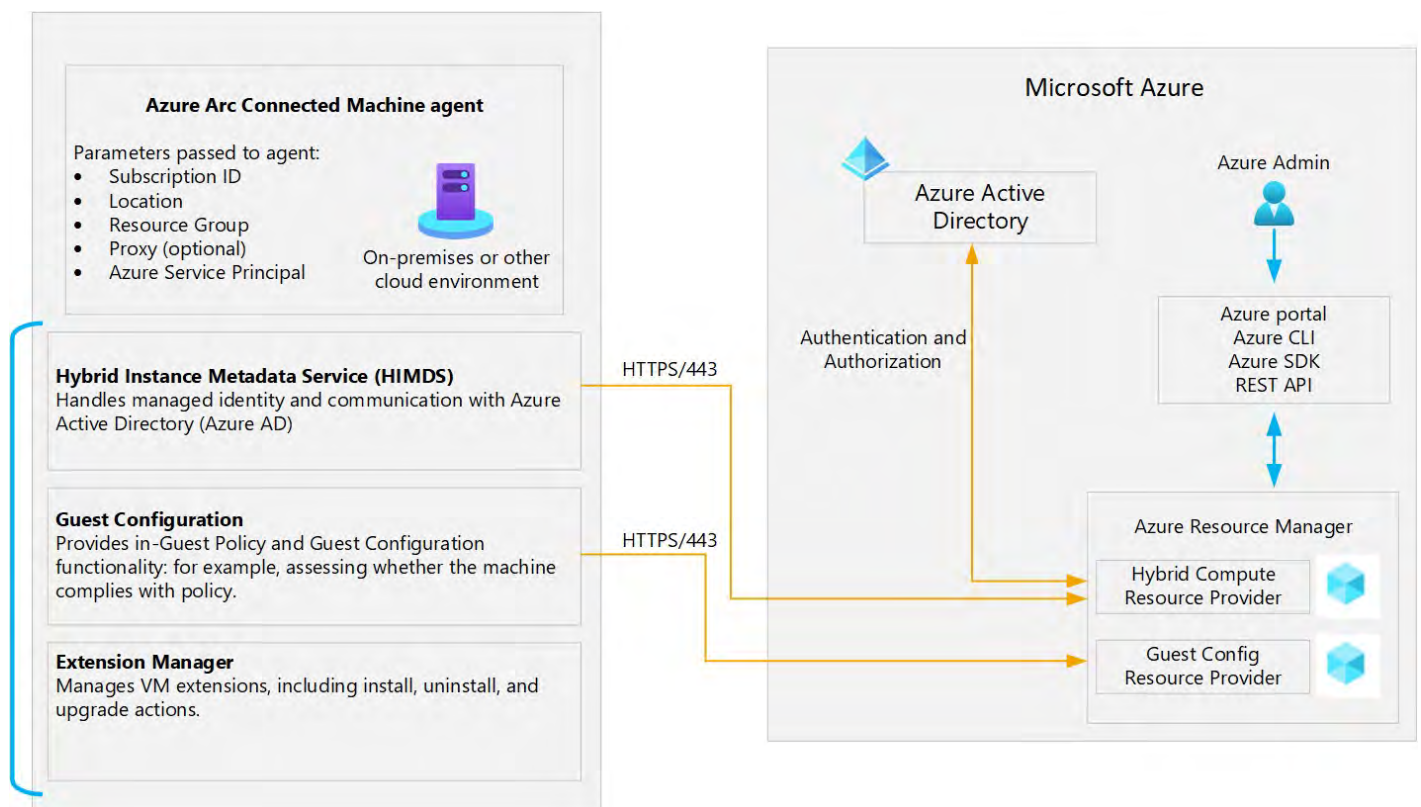
The Azure Resource Manager (ARM) was built as an extensible control plane and orchestration engine for Infrastructure-as-a-Service (IAAS) and, other managed services. Using ARM, we can manage and deploy resources using Infrastructure as a code paradigm. We can provision, modify, and decommission resources using built-in features, including access controls, tags, and locks with ARM. ARM provides us with a centralized dashboard that can integrate any Azure resources using third-party applications and services from the Azure marketplace. Centralized management console makes it simpler and easier since all resources are handled consistently.

Azure Arc is built on this foundation of ARM's extensibility feature. This extension of Azure Resource Manager, Azure Arc can support additional resources such as servers, Kubernetes clusters and databases, external resources, including Windows virtual machines, Linux virtual machines, Physical servers, databases, etc.



Onboarding Azure Arc Through Connected Machine Agent (Azcmagent)

The onboarding of Azure Arc is done by installing the Azure connected machine agent (Azure Arc agent) on the on-prem server. The Azure Arc agent can be installed on Windows Server or Linux hosts. Below is an illustration of how you can manage and maintain the Azure Connect Machine Agent (Azcmagent tool) for Azure Arc. This agent neither delivers any other functionality nor replaces the Azure Log Analytics agent. The Log and Analytics agent for Windows and Linux is required only if you wish to continuously monitor the operating system (OS).



Source: Azure Arc Connected Machine Agent Component details (Microsoft Docs)

Azure Connected Machine Agent Package has many Logical Components:

Hybrid Instance Metadata Service (HIMDS):

It is a Windows service that interfaces between the connection to Azure and the connected machine's Azure identity.

Guest Configuration Agent:

It provides in-guest policy and guest configuration functionality, such as checking whether the machine complies with the company policies or not.

Extension Manager:

The extension agent manages VM extensions, including install, uninstall, and upgrade. Extensions are extracted from the Azure site and downloaded to the folder.



Linux:

SystemDrive%\%ProgramFiles%\AzureConnectedMachineAgent\ExtensionService\downloads folder on Windows, and for Linux to /opt/GC_Ext/downloads



Windows:

On Windows, the extension is installed to the following path %SystemDrive%\Packages\Plugins\<extension>, and on Linux the extension is installed to /var/lib/waagent/<extension>

Note: The Azure Monitor Agent (AMA), currently in preview, does not replace the Connected Machine agent (Azcmagent). The Azure Monitor agent has replaced the Log Analytics agent, Diagnostics extension, and Telegraf agent for Windows/Linux machines. Check the Azure Monitor documentation about the new agent for more details.

Installing the Azure Connected Machine Agent:

To install the Azure Connected Machine agent (also known as Azure Arc agent) you have several different options.

Downloading the Agent from the Microsoft Repository:

Windows agent: Windows Installer package: Microsoft Download Center

The Linux agent package: Microsoft's package repository (using the preferred package format for the distribution (.RPM or .DEB))

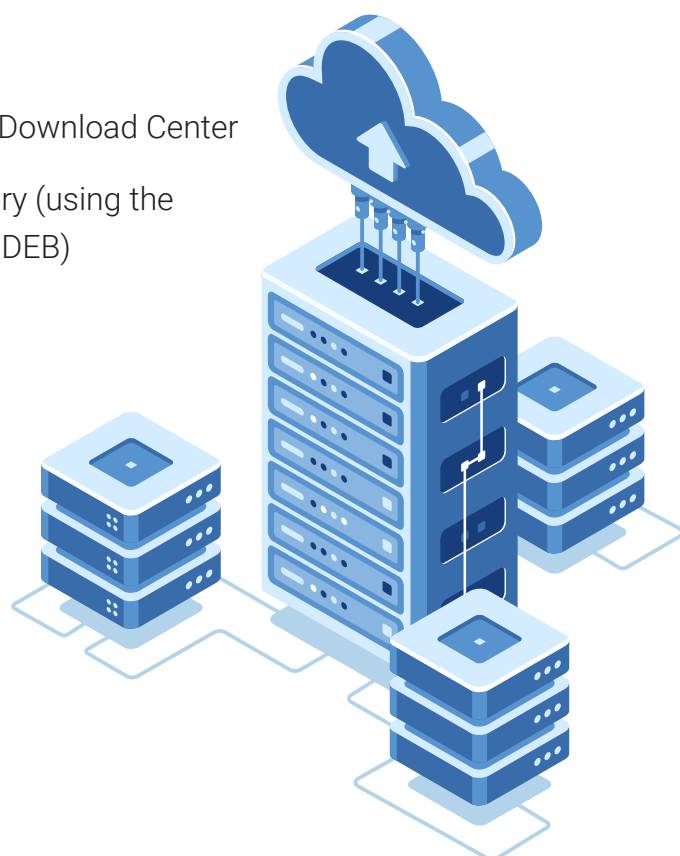
All we need to do is follow these two steps:

STEP 1.

Install the agent on the server

STEP 2.

Register the Azure-Arc enabled server with Microsoft Azure



The Azure Arc agent currently supports the following operating systems:



Linux:

- Ubuntu 16.04 and 18.04 LTS (x64)
- CentOS Linux 7 (x64)
- SUSE Linux Enterprise Server (SLES) 15 (x64)
- Red Hat Enterprise Linux (RHEL) 7 (x64)
- Amazon Linux 2 (x64)
- Oracle Linux 7



Windows:

- Windows Server 2008 R2, Windows Server 2012 R2, and higher (including Server Core)

Software requirements:

- .NET Framework 4.6 or later

Windows PowerShell 5.1 Permission requirements:

- The user ID needs to be a member of the Azure Connected Machine Onboarding or Contributor role in the resource group to onboard machines.
- To read, modify, and delete a machine, the user ID must be a member of the Azure Connected Machine Resource Administrator role in the resource group.
- To select a resource group from the drop-down list when using the Generate script method, at a minimum, your user ID needs to be a member of the Reader role for the particular resource group.

Network Requirement:

Connected Machine Agent for Windows and Linux communicates to Azure Arc over Transmission Control Protocol (TCP). Port 443 and 443 should be open on the installed server.

Please find the link to the JavaScript Object Notation (JSON) file of IP addresses for each service tag/region – <https://www.microsoft.com/en-us/download/details.aspx?id=56519>



Register Azure Resource Provider:

Azure Arc enabled servers depend on the following Azure resource providers in your subscription to use the service:

1. Microsoft.HybridCompute
2. Microsoft.GuestConfiguration

Azure PowerShell:

- Login-AzAccount
- Set-AzContext -SubscriptionId [subscription you want to onboard]
- Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute
- Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration

Azure CLI:

- az account set --subscription "{Your Subscription Name}"
- az provider register --namespace 'Microsoft.HybridCompute'
- az provider register --namespace 'Microsoft.GuestConfiguration'

Azure Portal:

- Sign in to the Azure portal(portal.azure.com)
- On the Azure portal menu, search for Subscriptions. Select it from the available options
- Select the subscription you want to view
- On the left menu, under Settings, select Resource providers
- Find the resource provider (Microsoft.HybridCompute/Microsoft.GuestConfiguration) you want to register and select Register

Configuring Connected Agent:

We can install the Azure Arc agent using two methods: Manual Installation and Automated installation.



Manual Install (Windows):

- Download the Agent tool from the website.
 - Run the installer package AzureConnected-MachineAgent.msi on the server.
- If the agent fails, check for logs in: %Program-Data%\AzureConnectedMachineAgent\log



Manual Install (Linux):

- Download the installation package by using:

```
wget https://aka.ms/azcmagent -O ~/Install_linux_azcmagent.sh
```
- Install the connected machine agent by using:

```
bash ~/Install_linux_azcmagent.sh
```

- Configure agent to communicate with Azure portal using the following command:

```
"%ProgramFiles%\AzureConnectedMachineAgent\azcmagent.exe"connect
--resource-group "resourceGroupName"
--tenant-id "tenantID" --location "region-Name" --subscription-id "subscriptionID"
```

- Configure the agent to communicate to portal by using the command:

```
azcmagent connect --resource-group
"resourceGroupName" --tenant-id "tenantID" --location "regionName" --subscription-id "subscriptionID" --cloud "cloud-Name" if [ $? = 0 ]; then echo "\033[33mTo view your onboarded server(s), navigate to https://portal.azure.com/#blade/Hub-sExtension/
```

Automated Installation (script-based):

- Open the Servers - Azure Arc page, and click on Add.
- On the Select a method page, click on the Add servers using interactive script tile and then click on Generate script.
- Open the Generate script page, click the subscription, and resource group where you want the machine to be managed within Azure. Provide an Azure location where the machine metadata will be stored. This location can be the same/different from the resource group's location.
- On the Prerequisites page, check the information and select Next: Resource details.
- On the Resource details page, perform the following:
 - On the Resource group list, select the resource group the machine will be managed in.
 - On the Region drop-down list, select the Azure region where the server's metadata is stored.
 - On the Operating system drop-down list, select the operating system that the script is supposed to run on.
- If the machine is communicating through a proxy server to connect to the internet, we need to specify the following: the proxy server's IP address or the name and port number that the machine will use to communicate with the proxy server. Example format **http://<proxyURL>:<proxyport>**.
- **Click Next:** Tags - On the Tags page, provide the default Physical location tags suggested and enter a value, or specify one or more Custom tags to support as per your requirements.
- **Click on Next:** Download and run the script.
- On the Download and run script page, verify the summary information, and click on Download. If you still need to make changes, click Previous and make the required changes.

Automated Windows Installation:

- Run the script downloaded above using PowerShell with administrator access. .

Automated Linux Installation:

- Access the server with an account that has root privileges. Change to the folder or share the one that has the script copied to and execute it on the server by initiating the `./OnboardingScript.sh` script.

Happiest Minds role in troubleshooting Azure Portal Connection Issue

Problem:

While working on a project, we had to deploy the Azure Arc agent on servers. We came across an on-premises virtual machine running windows 2012 OS shown as 'Offline' on the Azure Portal. However, the server was up and running fine without any issues in the on-premises data center.

Solution:

To help troubleshoot this, below are the steps we undertook.

● **Checking the Virtual Machine State** – First, verify if the virtual machine is running on the environment.

- Check if the VM is powered on and responding to "ping".
- Check if the VM can Remote Desktop Protocol (RDP) in case of Windows, and Secure Shell Protocol (SSH) in the case of Linux.

Many times various issues might occur that can cause a virtual machine to stop responding, including problems with the host. So, we should first check if the server is running smoothly.

● **Checking the Azure Arc for Servers State** – Azure Arc for servers uses an agent also known as a Connected machine agent. Check if the agent is installed on the server on Add/remove programs.

There should be a program installed by the name "Azure Connected Machine Agent". If it exists, then verify the services. Azure connected machine agent runs two services. The following services should be started, and in startup, type "automatic".

- Azure Hybrid Instance Metadata Service
- Guest Configuration Service

● **Checking the status of Azcmagent from command prompt** – Open command prompt as an administrator and run the following:

```
C:\Users\Administrator> Azcmagent show
```

```
C:\Users\Administrator>azcmagent show
level=fatal msg="Failed to communicate with Agent. Please make sure azcmagent is run with proper privileges, and that the service (Azure Hybrid Instance Metadata Service) is running." Error="open \\.\pipe\himds: The system cannot find the file specified."
```

The root cause could be that one of the services has stopped running. Possibly, the program was uninstalled accidentally or is being blocked by third-party security software that is preventing the service from running. It can also mean that the server has an underlying issue. Hence, we get the disconnected state on the Azure portal.

🟡 Double-check the prerequisites:

As mentioned above in the document, we need to verify a couple of prerequisites on the server. This includes supported operating systems, supported regions, Azure subscription, and service limits. Requirements are also listed on the Microsoft Docs Webpage.

There are no special ports required for communication as Azure Arc uses TCP port 443. Verify the ports by running "netstat -ano findstr 443".

If the firewall is restrictive as per the existing infrastructure, we will check if the Azure URL's/IP ranges and services tags are allowed.

🟡 Issuing a reconnect command:

If the server was connected previously and was working, we can use the Azcmagent tool to administer a reconnect command.

This would be useful if the server has been powered off for more than forty-five days and its local certificate has expired, but the VM still appears on Azure Arc blade.

The steps mentioned below will require you to validate your Azure credentials in the form of a service principal access token/Azure login screen. Running the command will re-direct you to visit your Azure login page.

To reconnect the agent, you can use the command below:

azcmagent reconnect --tenant-id <tenantID>

The preferred method however is to use Service Principal ID which requires you to provide the information given below:

azcmagent reconnect --service-principal-id <serviceprincipalAppID> --service-principal-secret <serviceprincipalPassword> --tenant-id <tenantID>

This command worked in our case, and we could initiate a new connection to the Azure portal. Appended is the response we got when we ran the command "azcmagent show".

```
C:\Users\Administrator>azcmagent show
Resource Name      : BNE02
Resource Group Name : BNE-Core
Subscription ID    : 
Tenant ID          : 
VM ID              : 
Location           : westus2
Agent Version      : 0.7.20079.002
Agent Logfile      : C:\ProgramData\AzureConnectedMachineAgent\Log\himds.log
Agent Status       : Connected
```

- **Disconnect and Connect (Optional):**

Additionally, we can disconnect and connect again using the following commands:

```
azcmagent disconnect --service-principal-id <serviceprincipalAppID> --service-principal-secret <serviceprincipalPassword> --tenant-id <tenantID>
```

```
azcmagent connect --service-principal-id <serviceprincipalAppID> --service-principal-secret <serviceprincipalPassword> --tenant-id <tenantID> --subscription-id <subscriptionID> --resource-group <ResourceGroupName> --location <resourceLocation>
```



Conclusion

Azure Arc for Server brings the cloud to their customers instead of directing the customers to the cloud. It is a robust governance solution that everyone can avail of free of cost for monitoring, managing, and keeping a tab on their on-premises resources, just like their infrastructure on Azure cloud, under a single plane.

With Azure Arc, customers can now see the benefits of launching new cloud products, including up-to-date data capabilities, use in seconds (instead of hours), and flexibility in any infrastructure. From the Azure portal, customers get a seamless and consistent view of all Azure data services operating locally and, in the cloud, apply consistent policies, security and data management, and more. Additionally, when it comes to DevOps operating models and IT Operations, they are challenging to use, as existing tools fail to support new native cloud patterns. Azure Arc can simplify administration and management overhead by delivering a cloud-based static and administrative platform from a single plane on Azure.



Navneeth

has over 15+ years of experience handling Azure cloud, windows platform, and datacenter management. He has spent many years in the IT infrastructure industry with expertise in migration, monitoring, and consulting on-premises servers to the cloud. Currently, he is part of Azure practice in Happiest Minds as Senior Technical Lead. Key responsibilities of this role include planning and implementing heterogeneous migration on Cloud/On-Prem Infrastructure.



Business@happiestminds.com

Happiest Minds Technologies Limited (NSE: HAPPSTMNDS), a Mindful IT Company, enables **digital transformation** for enterprises and technology providers by delivering seamless customer experiences, business efficiency and actionable insights. We do this by leveraging a spectrum of disruptive technologies such as: **artificial intelligence, blockchain, cloud, digital process automation, internet of things**, robotics/drones, **security, virtual/augmented reality**, etc. Positioned as 'Born Digital . Born Agile', our capabilities span digital solutions, infrastructure, product engineering and security. We deliver these services across industry sectors such as automotive, BFSI, consumer packaged goods, e-commerce, edutech, engineering R&D, hi-tech, manufacturing, retail and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, Canada, Australia and Middle East.

www.happiestminds.com