eG Innovations

How to Monitor Azure Virtual Desktop (AVD) Technology

An eG Innovations Technical White Paper

www.eginnovations.com

❖ Introduction

Azure Virtual Desktop (AVD) technology is growing in popularity as a means of delivering virtual desktops in the cloud to users. *A recent eG Innovations and AVD TechFest study* found that 26% of organizations already have AVD deployed and within two years, almost 84% of all organizations will be using AVD technology in production in one form or the other.

One question many administrators are asking is: How can I effectively and efficiently monitor AVD? There are several options for monitoring AVD and this whitepaper will cover some of the most popular ones.

❖ What is Azure Virtual Desktop?

Azure Virtual Desktop (AVD), previously known as Windows Virtual Desktop (WVD) is a flexible cloud virtual desktop infrastructure (VDI) platform hosted on Microsoft Azure that securely delivers virtual desktops and remote apps with maximum control. Its capabilities include:

- Windows 10 and Windows 11 personalized and multi-session desktops and remote app streaming
- Full control over management and deployment, plus options for Citrix and VMware integration
- Flexible consumption-based pricing

AVD is a free service for Microsoft customers with most types of Windows 10/11 Enterprise licensing. However, the subscription or pay as you go (PAYG) Azure costs are additional. Likewise, the cost for many monitoring components you may wish to add such as Log Analytics and Azure Monitor is also additional.

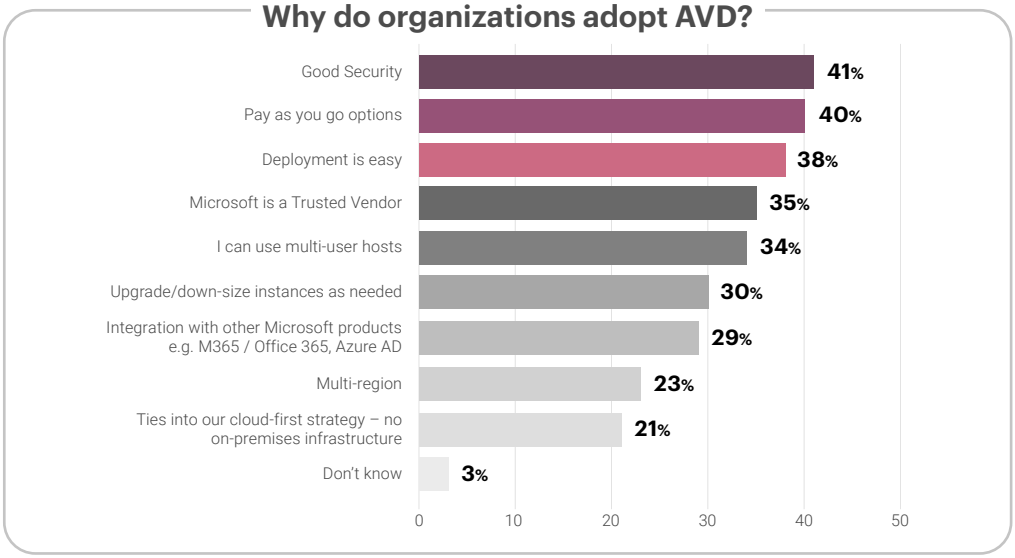


Figure 1: Main reasons for AVD adoption

Figure 1 highlights some of the main reasons for AVD adoption and growth in popularity. In part, AVD adoption was driven by the COVID pandemic. Demand for DaaS (Desktop-as-a-Service) grew to support remote work and work from home. Beyond this, AVD has gained customers who have moved from competing alternatives because of its ease of deployment, PAYG model and unique feature offering for Windows 10/11 including multi-session desktops and tight integration with other Microsoft offerings such as Microsoft 365 (Office 365).

❖ Virtual Desktops on Azure: Different Provisioning Models

Virtual desktops can be provisioned on Microsoft Azure cloud in different ways.

- One of the popular ways of providing virtual desktops has been by deploying Windows servers on Azure and brokering user sessions to these servers using a Citrix or Omnissa Horizon control plane.
- Another option is to deploy Windows 10/11 workstations on the cloud and have them brokered by Citrix or Omnissa Horizon or natively by Microsoft Azure.
- While both the above options have been available for several years, the most recent addition has been the ability to provision multiple user sessions on a Windows 10/11 host. Previously, this could only be achieved on Windows server operating systems. This capability gives users a familiar Windows 10 experience while IT can benefit from the cost advantages of multi-session and use existing per-user Windows licensing instead of RDS Client Access Licenses (CALs). For more information about licenses and pricing, see *Azure Virtual Desktop pricing.* You can learn more about multi-session Windows hosts here: *https://docs.microsoft.com/en-us/azure/virtual-desktop/windows-10-multisession-faq*

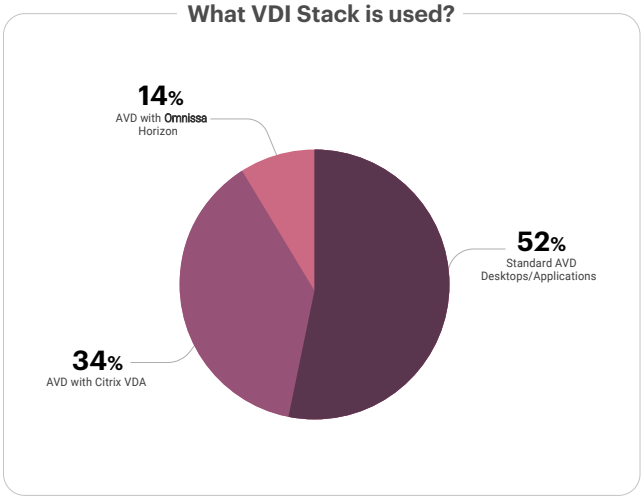


Figure 2: Customers choose between Citrix VDAs, Horizon desktops and native Azure desktops

As you can see from Figure 2, currently, just over 50% of organizations are using the native Microsoft stack. This number is expected to increase as multi-session AVD adoption grows.

In this whitepaper, we will focus on multi-session, native Azure virtual desktops. Since Citrix and Omnissa Horizon have been adopted for several years, monitoring capabilities and best practices for these technologies are well documented in other eG Innovations *whitepapers* and *blogs.*

Citrix and Omnissa Horizon vs. AVD

Is AVD a competitor to Citrix or Omnissa Horizon? The answer is not clear cut. It's a combination of Yes and No. The eG Innovations and AVD Tech survey of AVD adoption found that AVD is being adopted by smaller businesses. 73% of AVD deployments were supporting less than a thousand users.

In contrast, Citrix and Omnissa Horizon are typically adopted by mid to large sized organizations. Organizations using a mix of on-premises and cloud environments may also prefer a Citrix or a Omnissa Horizon stack.

A *recent Citrix blog* provides a good summary of the value addition offered by Citrix brokering technology over native Azure virtual desktop technology.

❖ The Architecture of AVD

To understand what is needed to monitor AVD technology, it is important to understand the AVD architecture (see Figure 3):

- The endpoints used to access AVD are in the customer's network. ExpressRoute extends the on-premises network into the Azure cloud, and Azure AD Connect integrates the customer's Active Directory Domain Services (AD DS) with Azure Active Directory (Azure AD).
- The AVD control plane handles Web Access, Gateway and Connection Brokering functionality.
- The session hosts used to host user sessions are provisioned as VMs in an Azure subscription. Host pools are a collection of one or more session hosts. Each host pool can contain an app group that users can interact with as they would on a physical desktop.
- Storage is usually provided using Azure Files or Azure NetApp Files.

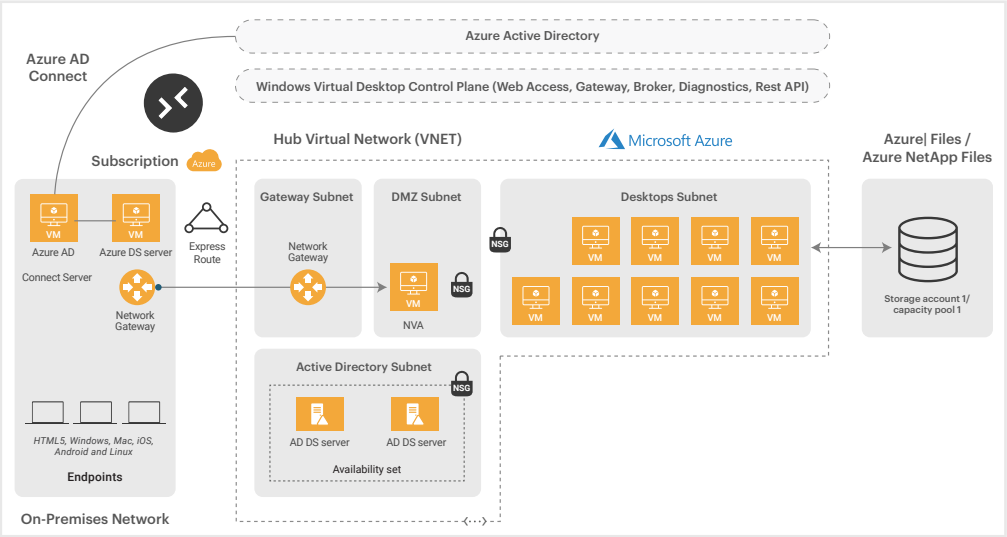


Figure 3: Microsoft AVD Architecture

❖ Four Big Challenges When Monitoring AVD

While AVD technology is simple to provision, it can be quite challenging to monitor, troubleshoot and operate. There are many reasons for this:

- With on-premises technologies like Citrix and Omnissa Horizon, the IT team had complete control over every layer and every tier of the infrastructure, servers, storage and other technologies supporting the digital workspace service. With AVD, the underlying infrastructure is controlled by Microsoft. The applications being accessed may also be under the control of a different service provider. This means that **IT teams have to troubleshoot AVD problems with limited visibility.**

- AVD deployments are often more distributed than on-premises digital workspaces. The applications being accessed and the virtual desktop that the user is connected to could be in different geo locations. Even for authentication, synchronization between AD Connect in the cloud and an on-premise AD is required. **The distributed nature of AVD makes monitoring more challenging.**

- **The pay-as-you-go model of AVD means that cloud costs increase with usage.** Tracking any wasteful resource usage and providing recommendations for optimization also falls under the scope of monitoring technologies.

- Like other digital workspace technologies, AVD is extremely performance sensitive since users are connecting to their digital workspaces from remote locations, with limited resources on the client and often their network. When a problem happens, **it is a challenge to determine where the cause of the problem lies:** is it with the user's network, with the application being accessed, a bottleneck with Azure resources, an Active Directory issue, etc.

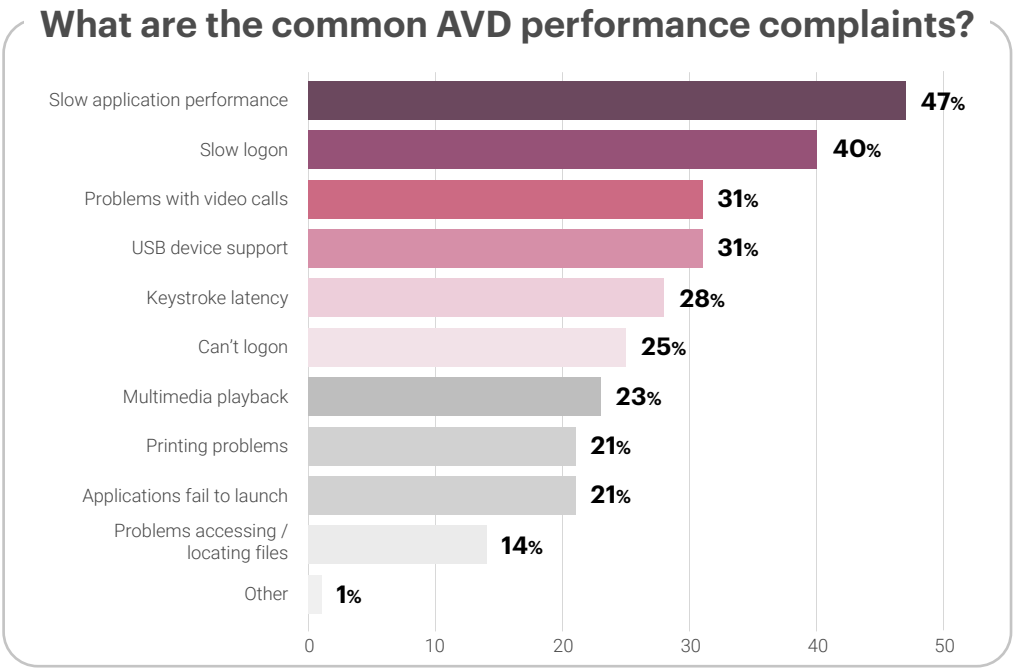


Figure 4: Common AVD performance complaints that IT admins receive

What SLAs does Microsoft provide

A significant attraction of Microsoft Azure is Microsoft's commitments via service level agreements (SLAs) to high-availability and uptime with most Azure services guaranteeing availability 99.9% of the time or higher. For AVD itself though Microsoft does not offer a financially backed SLA and the commitment is to *"strive to attain at least 99.9% availability for the Azure Virtual Desktop service URLs"*. The availability of the session host virtual machines in your subscription is covered by the Virtual Machines SLA.

❖ 10 Questions an AVD Monitoring Tool Must Answer

Before you begin your search for an AVD monitoring tool, you must be able to answer these key questions. Having ongoing access to the answers to these performance-related questions will mean that you can troubleshoot problems faster, reducing MTTR, spot problems before they impact end-user experience, and empower your helpdesk.

- Like all digital workspace technologies, the success of AVD is measured by user experience. Hence, the first question to answer is what is the user experience for desktop users? Is the AVD service available throughout and how long does it take to access a desktop?
- Getting logon to work is like getting to make a call or receive a call on your phone. Hence, a key question is whether AVD logon is working and how long does it take for a user to login? If the logon time is high, why is it so high?

- Once a user is connected to their virtual desktop, if access is slow, it will affect user productivity. Is there any lag or latency during user access? Are there any packet losses or retransmissions while the session is in progress?
- What is the resource usage level on the session hosts that the users are connected to and is there a resource constraint on the hosts?
- Are there many disconnected sessions (i.e., sessions taking up resources that do not have an active user) on the session hosts?
- Is the workload balanced and distributed evenly across all the session hosts?
- Is any session host idle (i.e., there is cost wastage), and is any session host without a heartbeat (i.e., can't get any new sessions)?
- Are there any connection failures occurring to the AVD service?
- Has any unusual sign-in activity been detected through Azure AD?
- Are there sufficient session hosts to handle the workload, or do you need to provision additional capacity?

These are just some of the many questions that an administrator is likely to need instant access to whilst tracking and monitoring the performance of an AVD deployment and the digital experience of its users.

❖ 4 Key Capabilities Your AVD Monitoring Tool Must Have

The eG Innovations AVD TechFest survey on AVD adoption found that the most frequently reported challenge in an AVD deployment is end user experience. **Hence, the ability to monitor user experience of AVD users is the most important capability of your AVD monitoring tool.** A degree of user experience monitoring can be performed using synthetic transactions – i.e., simulating a user logging in and accessing AVD. This must also be complemented by monitoring real users to understand, prevent and respond to real end user issues effectively. Ideally, your AVD monitoring solution must support both synthetic and real user monitoring (RUM).

When user experience is poor, for example if logon times are 2 mins, the immediate question is why is AVD user experience poor? Answering this question without comprehensive monitoring is difficult. Sometimes the issue could be in Active Directory, sometimes it could happen because the storage tier is slow, or it could be because the FSLogix profile management container has not been attached. Hence, **monitoring of every layer and every AVD tier is important.**

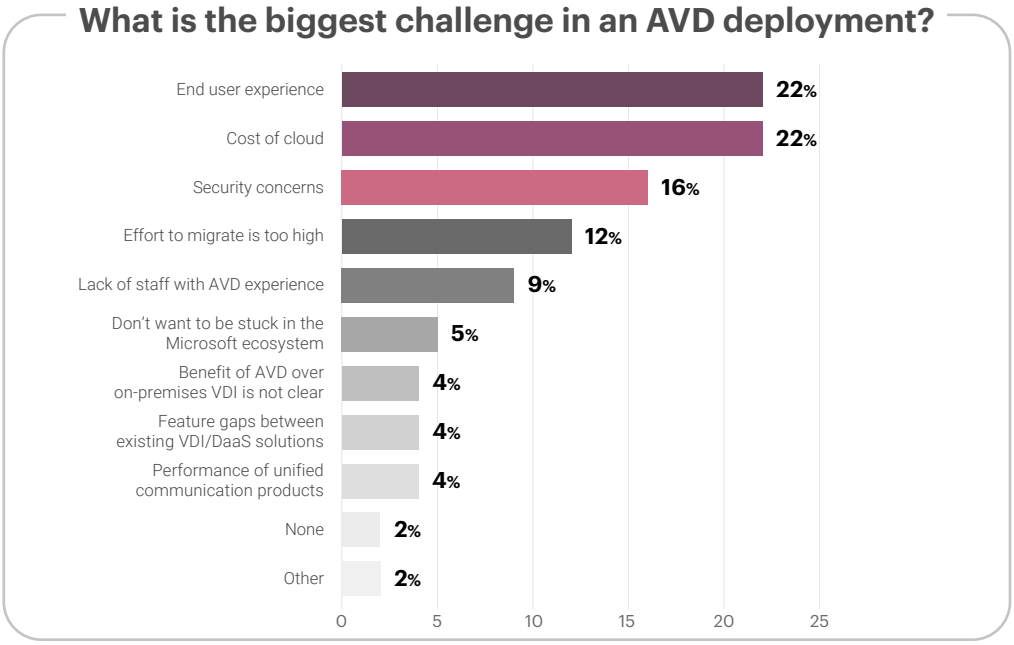


Figure 5: 4 Key challenges IT admins face when deploying AVD

- This means monitoring the AVD session hosts alone is simply not sufficient . Every AVD tier – i.e., the AVD broker, the Azure AD, network connectivity, Azure subscription, etc. – must also be monitored.

When monitoring an AVD deployment with hundreds of concurrent users, a comprehensive monitoring tool should be expected to collect several thousands of metrics. Analyzing these metrics manually would be time consuming, cumbersome and unfeasible. AVD monitoring tools need to be able to analyze thousands of real time metrics at scale on near instant timeframes. They **must embed AIOps capabilities that use machine learning** to analyze metrics and highlight where the abnormalities lie. Ideally, analyzing the dependencies of an AVD service, the monitoring tool **should be able to do root-cause analysis and pin-point where the real problems lie,** so IT admins can focus on root causes and not be distracted by the secondary symptomatic effects. Effective automated correlation and alert filtering is essential to prevent alert storms and time-wasting false positives.

Finally, cost can be a significant concern and barrier to wide-spread AVD adoption. **AVD monitoring tools should have embedded intelligence to detect abnormal usage patterns, wasted resources, insufficient provisioned capacity,** etc. and provide recommendations, so IT admins can optimize their AVD deployments for maximum performance at minimal cost.

❖ What Tools Can You Use to Monitor Azure Virtual Desktop Technology

Azure Virtual Desktop adoption is still in the nascent stages and a relatively new digital workspace technology, so there are not the variety of tools to monitor AVD as there are *monitoring tools for Citrix.* There are two main options at the moment: *Azure Monitor,* which is the native cloud monitoring service from Azure, or a third-party tool like *eG Enterprise.*

Using Azure Monitor for AVD Monitoring

Azure Monitor

Azure Monitor for Azure Virtual Desktop includes a simple dashboard built on Azure Monitor Workbooks that helps IT professionals understand their Azure Virtual Desktop environments. Before you start using Azure Monitor for AVD, you will need:

- At least one Log Analytics Workspace configured. It is recommended to use a designated Log Analytics workspace for your Azure Virtual Desktop session hosts to ensure that performance counters and events are only collected from session hosts in your Azure Virtual Desktop deployment.
- To enable data collection for the following things in your Log Analytics workspace:
  - Diagnostics from your Azure Virtual Desktop environment
  - Recommended performance counters from your Azure Virtual Desktop session hosts
  - Recommended Windows Event Logs from your Azure Virtual Desktop session hosts

You will also need to provide:

- Read-access to the Azure resource groups that hold your Azure Virtual Desktop resources
- Read-access to the subscription's resource groups that hold your Azure Virtual Desktop session hosts
- Read access to the Log Analytics workspace or workspaces

To access Azure Monitor for Azure Virtual Desktop, you can Search for and select **Azure Virtual Desktop** from the Azure portal, then select **Insights.**

- Note: Setting up Azure Monitor to monitor multiple subscriptions is not straightforward. You would set up a Log Analytics workspace to monitor resources in all of your subscriptions as long as they are under the same Tenant. If you have multiple Azure AD Tenants, like an MSP would, you will need to use *Azure Lighthouse* to see all subscriptions under your main tenant.

The various steps involved in setting up Azure Monitor for AVD are explained here: *https://docs.microsoft.com/en-us/azure/virtual-desktop/azure-monitor*

Log Analytics and Azure Monitor are additional paid for services that together are often used to implement a basic level of monitoring, reporting and alerting. A Log Analytics workspace is a unique environment for Azure Monitor log data. Each workspace has its own data repository and configuration, and data sources and solutions are configured to store their data in a particular workspace.

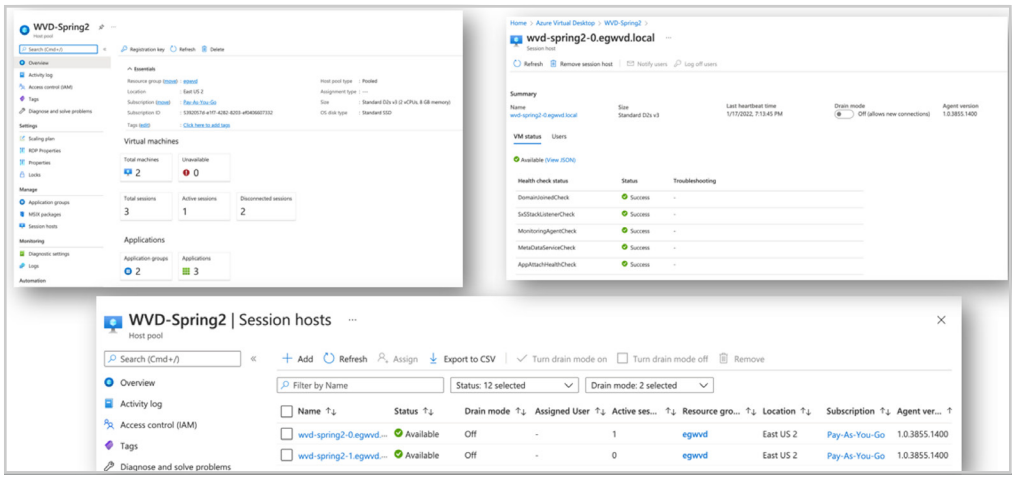


Figure 6: Azure Monitor can be used to get overview and details of AVD performance

With Azure Monitor, you can monitor all key AVD metrics. You can select any of the collected metrics and see charts and graphs over time. Alerting capabilities are also available but need to be configured either manually or via bespoke scripting requiring in-house development.

Billing is based on data ingested and also on the storage for any data retained beyond the default 30-day retention period. Alerting is also an additional cost billed per alert threshold set. Costs vary depending upon the alert type used (static vs. dynamic).

Common Challenges that AVD admins highlight with Azure Monitor

There are many challenges with using Azure Monitor for AVD monitoring:

- Setting it up involves a lot of manual effort, especially around what metrics to collect, what thresholds to set, when to get alerts, etc.
- Difficult to estimate cost, especially the costs of monitoring as this depends on many factors – number of metrics, types of thresholds, etc.
- Integration with other ITSM tools and enterprise workflows is not straightforward.
- Many a time, AVD admins have to write Kusto queries to generate reports they need.
- Azure Monitor is designed as a tool for the AVD administrator. It is not simple enough that it can be used by help desk operators and does not restrict functionality or visibility sufficiently to allow help desk safe controlled access within a security conscious organization.
- Free-form text fields (e.g., for naming alerts) make it hard to enforce standards and conventions and ensure human readable information is available.
- Very often, AVD is deployed along with other digital workspace technologies such as Citrix and VMware. Azure Monitor cannot be used for monitoring these technologies and hence, separate consoles are needed for Citrix and Omnissa Horizon monitoring.
- Azure Monitor has no built-in synthetic monitoring capabilities for AVD.

Using eG Enterprise for AVD Monitoring

eG Enterprise is a specialized monitoring solution for both cloud and digital workspace environments. With over a decade of experience supporting some of the largest digital workspace deployments, eG Enterprise includes out-of-the-box dashboards and reports that typical AVD admins need.

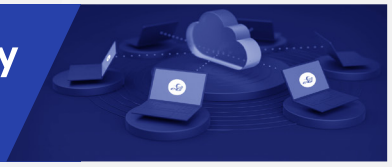
- **There is little configuration required.** Just install agents on your session hosts and your host pool and its hosts are auto-discovered and monitored, even when leveraging auto-scaling technologies.
- **All user sessions are tracked at a granular level** and all aspects of user experience are monitored for every session. This includes Windows logon time, breakdown of time spent into GPO processing, FSLogix processing, connection brokering, input delay for the session, round trip time (RTT) latency, packet loss and retransmissions, application launch time, etc.
- **Synthetic monitoring is also supported** so AVD admins can track performance of the service 24x7 and be proactively notified of any problems with desktop access or slowness.
- Besides monitoring the session hosts, eG Enterprise also monitors the AVD brokering service, Azure AD, Azure Subscription, Azure AD Connect and so on. This way it can **provide an end-to-end topological view of the AVD service.**
- **AIOps capabilities embedded in the solution** help with proactive alerting and alarm correlation to pinpoint the cause of problems. Out of the box, the solution has the top 20+ reports that AVD admins need pre-built.

Enabling Proactive Detection and Resolution of Common AVD Problems

The toughest problem that any IT administrator has to deal with is when a user calls with a complaint that their virtual desktop or application "is slow". There can be several reasons why this could happen in an AVD environment. Some of the common reasons include:

- Azure outages
- Storage failures
- FSLogix attachment issues
- Disk space issues with FSLogix
- NIC issues on the hosts
- Under-sizing of session hosts
- Excessive resources consumed by one user
- Memory leak in an application
- Issues connecting to Azure AD
- Session hosts that are disconnected from Azure control plane
- Auto-scaling of session hosts fails to occur

eG Enterprise's out of the box monitoring for AVD includes rapid diagnosis and solutions to these common AVD problems.



Azure Monitor for AVD vs. eG Enterprise – A Quick Comparison

Azure Monitor	eG Enterprise
Significant manual effort to set up especially around what metrics to collect, what thresholds to set, when to get alerts, etc.	Minimal manual effort. Metrics to be collected, thresholds to set are pre-defined.
Difficult to estimate cost – every alert costs money; pricing is different for different types of thresholds. Amount of data collected and historical storage also increases the cost.	Easy to estimate cost. Licensing is based on number of users.
Possible to monitor multiple subscriptions but more complex to configure. Subscriptions within a tenant can be configured in a single log analytics workspace. Monitoring resources across tenants requires Azure Lighthouse.	Easy to configure to monitor multiple Azure subscriptions.
Cannot be used to monitor Citrix, Omnissa Horizon, or other digital workspace deployments like AWS AppStream or WorkSpaces.	Provides consistent dashboards and reports across all popular digital workspace technologies including Citrix, Omnissa Horizon, AWS AppStream and others. Licensing transferable between workspace technologies.
Supports basic HTTP URL checks for availability. Multi-step web tests are supported with the help of Azure Application Insights. Does not include built-in simulators for AVD or other digital work-spaces. Does not have full session monitoring for thick / thin clients.	Extensive in-built synthetic monitoring capabilities ranging from simple protocol checks to logon simulators for AVD and other digital workspaces to full session monitoring for thick, thin or web clients.
Report generation involves writing Kusto queries.	Simple reporting interface includes a number of pre-built reports. Customized reports can also be created. Users do not have to invest in Kusto skills and do not need to write queries.
Interface more suited to admins than helpdesk staff. Root-cause diagnosis and analytics are left to other tools that take feeds from Azure Monitor.	Role-based access and personalized views are supported. Helpdesk staff can easily navigate the interface and triage problems quickly.
Integration with ITSM tools and enterprise workflows is difficult. Manual configuration is needed.	Many out of the box integrations are available for supporting most common ITSM tools including Autotask, ServiceNow and others.

❖ How eG Enterprise Addresses the Key Monitoring Needs of AVD Deployments

Synthetic Monitoring of AVD Logon Performance and User Experience

User experience monitoring is one of the key needs for AVD admins. eG Enterprise includes a purpose built logon simulator for AVD. This browser-based tool is deployed on a dedicated VM/desktop and periodically logs into the Azure portal, launches the published desktop or application, waits for the desktop or application launch to complete and reports the success/failure of the logon attempt and the time taken for the simulation.

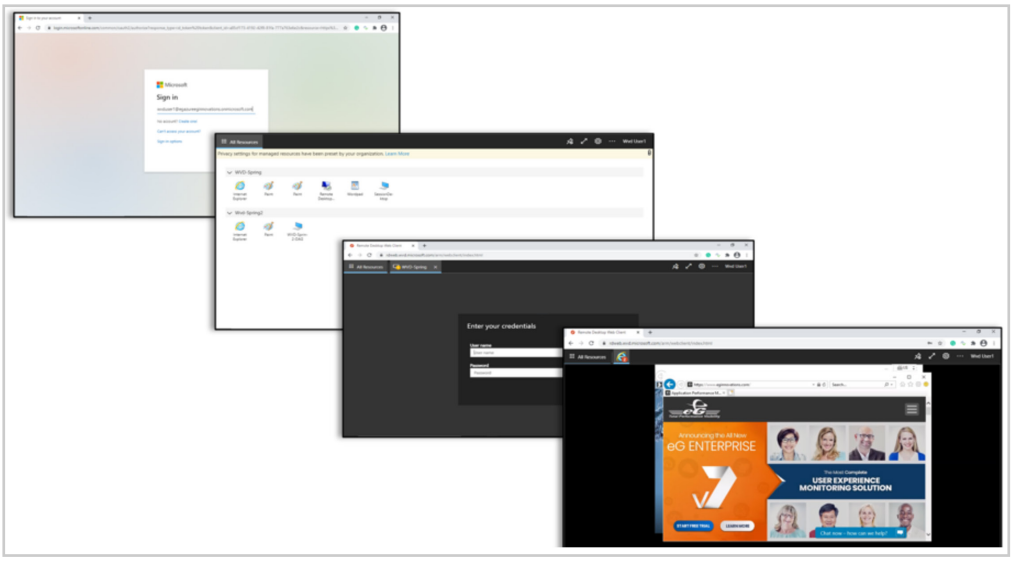


Figure 7: AVD logon simulation with eG Enterprise

Simulations can be performed using different accounts (e.g., different departments using AVD), and from different locations (e.g., branches). The simulations can run 24x7 and can proactively alert IT admins to potential issues with the AVD service in advance of real users encountering logon issues.

Figure 8 shows a dashboard, highlighting the results of logon simulation of AVD. In the top part of the figure, each row is a simulation. The results of the simulation are color coded. Red color highlights problems when they happen. Clicking on each row shows details of the simulation.

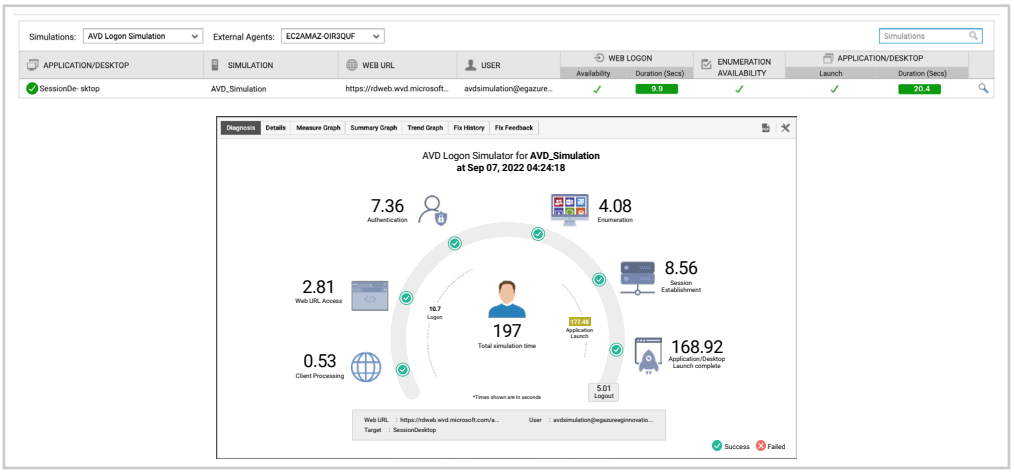


Figure 8: Dashboard showing the results of AVD Logon Simulation

The details in the bottom half of Figure 8 highlight the time spent during simulation in each stage: opening the browser, accessing the Microsoft portal, authenticating the user, checking if the application/desktop is enumerated (i.e., present on the page and can be accessed), session establishment with the session host and application/desktop launch. The timing associated with each step can provide an indication of where slowness may arise from. For example, if authentication is slow, there could be a problem with Azure AD, and if application/desktop launch is slow, the issue could be due to a faulty GPO or a large profile, or an FSLogix issue.

Logon simulation is the easiest way to get started with monitoring AVD. If you want to simulate AVD logons using a native client application (not a browser) or if you need to simulate user interactions beyond logon (e.g., accessing an application, logging into it, doing work in the application and then logging out), logon simulation is not sufficient. Full session simulation in eG Enterprise supports this functionality. The workflow to be simulated must be recorded by the admin using a recording tool and then a playback tool takes care of periodically replaying the scripted actions. Figure 9 below shows a dashboard depicting the real-time status of a simulated workflow.

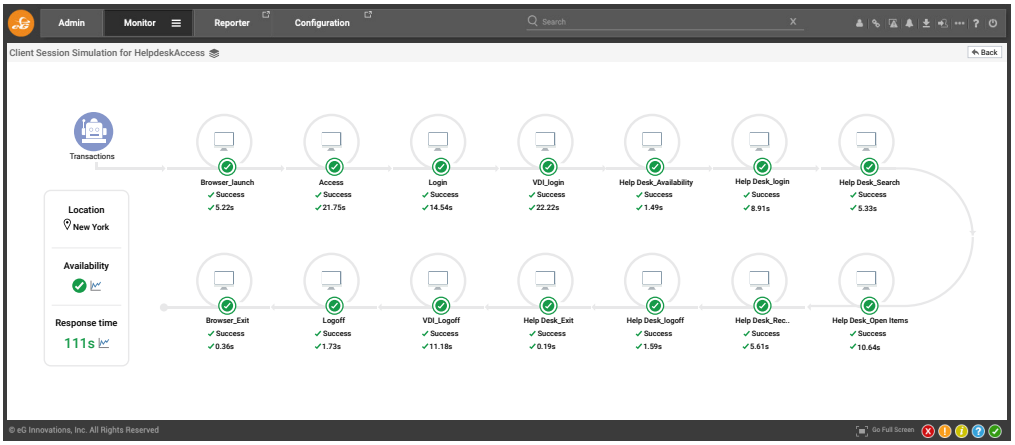


Figure 9: Full session simulation showing the performance of each step of the simulated workflow

Real User Experience Monitoring (RUM) for AVD

Synthetic monitoring alone is insufficient to proactively avoid users encountering issues or troubleshoot any issues real users encounter. After all, synthetic monitoring is performed from a limited set of locations and using a small set of user login accounts with standardized workflows. Hence, monitoring of real user activities and their experience when accessing their applications and desktops is important.

Users connect to the Azure control plane and are assigned to one of the session hosts in a host pool. Since most of their activities during a session occur on a session host, user experience for a user's session is best monitored using agents on each session host. The agent on a session host monitors various aspects of AVD user experience:

- **Windows logon duration monitoring:** Windows logon happens on the session host. The user is authenticated, their profile is loaded, GPOs are processed, etc. The eG agent on a session host tracks all of these activities and reports the total logon processing time on the session host.

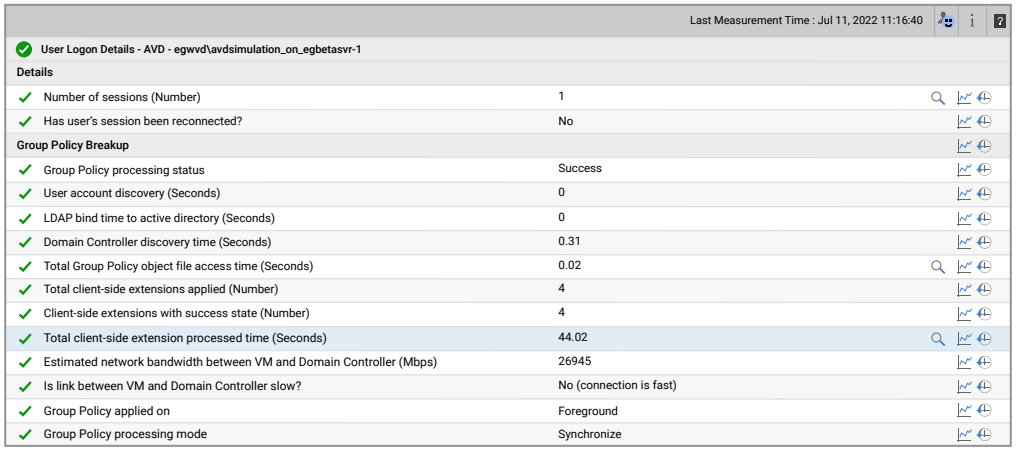


Figure 10: Monitoring of user logon on a session host

The time taken for each GPO (Group Policy Object) processed is also tracked so if a particular GPO is slowing down a user's logon, eG Enterprise can easily highlight it. Data is available with the granularity of individual CSE (Client-side Extension). Also note that the success/failure of GPO processing and the error code, if any, are also monitored, so administrators can easily see if GPO processing is causing AVD logon issues.

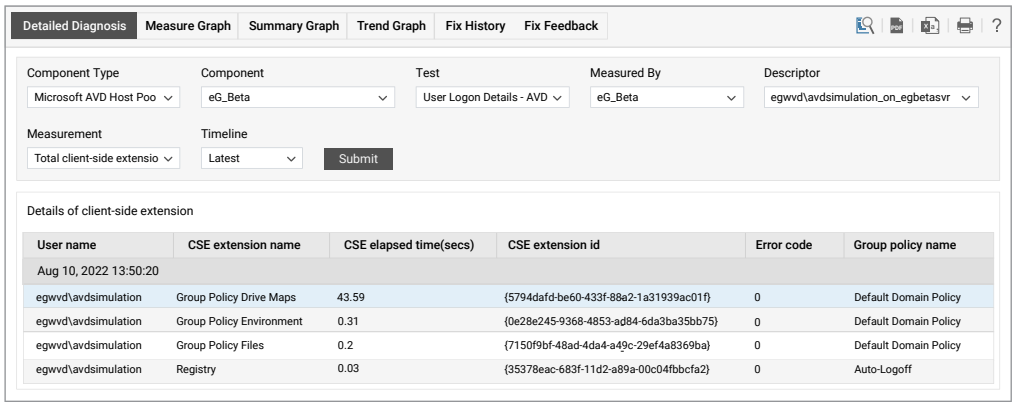
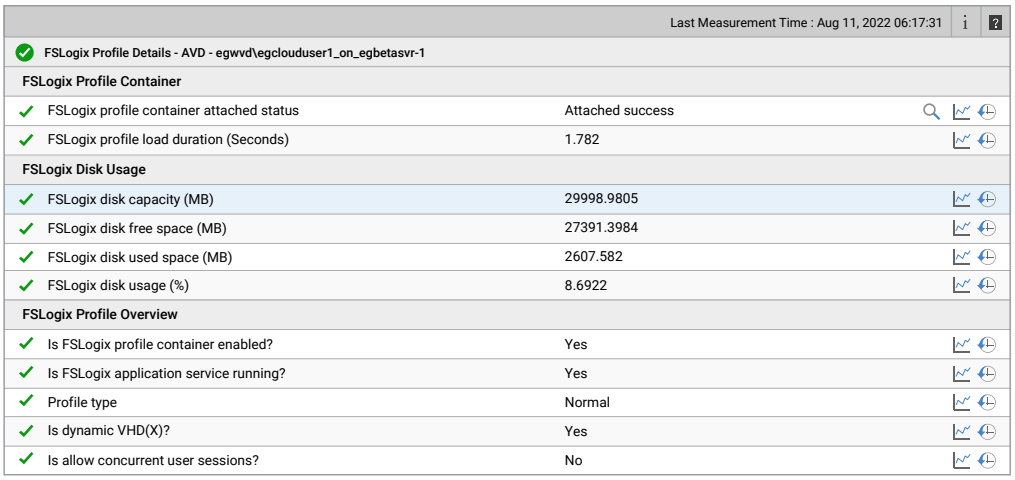


Figure 11: Details of GPOs processed when a user logs on to a session host

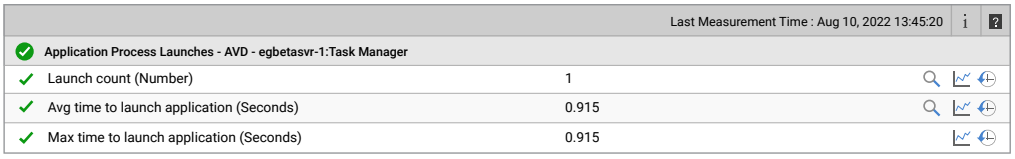
AVD includes the free use of FSLogix containers for profile management. If an FSLogix disk is not attached during user logon, the user's profile may not be available. eG Enterprise's monitoring of AVD reports the status of the FSLogix profile container – whether it is attached or not. Space usage on the container is also tracked and excessive usage is highlighted and alerts raised.



Last Measurement Time : Aug 11, 2022 06:17:31		
FSLogix Profile Details - AVD - egwvd\egclouduser1_on_egbetasvr-1		
FSLogix Profile Container		
FSLogix profile container attached status	Attached success	
FSLogix profile load duration (Seconds)	1.782	
FSLogix Disk Usage		
FSLogix disk capacity (MB)	29998.9805	
FSLogix disk free space (MB)	27391.3984	
FSLogix disk used space (MB)	2607.582	
FSLogix disk usage (%)	8.6922	
FSLogix Profile Overview		
Is FSLogix profile container enabled?	Yes	
Is FSLogix application service running?	Yes	
Profile type	Normal	
Is dynamic VHD(X)?	Yes	
Is allow concurrent user sessions?	No	

Figure 12: Monitoring of FSLogix profile management status and performance for a user's session

- **Application launch time monitoring:** Slowness can occur when a user clicks on an application and it takes excessive time for the application to launch and be available for user interaction. An eG agent reports this application launch time for any interactive application accessed by users. By tracking this metric, you can determine if a specific application is slow to launch, or if all applications are slow to launch on a session host, etc.



Last Measurement Time : Aug 10, 2022 13:45:20		
Application Process Launches - AVD - egbetasvr-1:Task Manager		
Launch count (Number)	1	
Avg time to launch application (Seconds)	0.915	
Max time to launch application (Seconds)	0.915	

Figure 13: Tracking launch time of applications on a session host

- **Protocol performance monitoring:** When a user is in a session, latency and bandwidth are key metrics that determine whether the user perceives the virtual application or desktop to be responsive. The eG agent on a session host tracks frame quality, packet loss during transmission, retransmissions and bandwidth used for each user session for all major protocols including RDP and RemoteFX. Frames skipped are indicative of performance degradations and the eG agent reports if frames are skipped on the client, on the server or in the network, which gives admins an idea of where the bottlenecks are. For example, if frames are skipped on the client, it is a user-end issue, not in the AVD infrastructure.

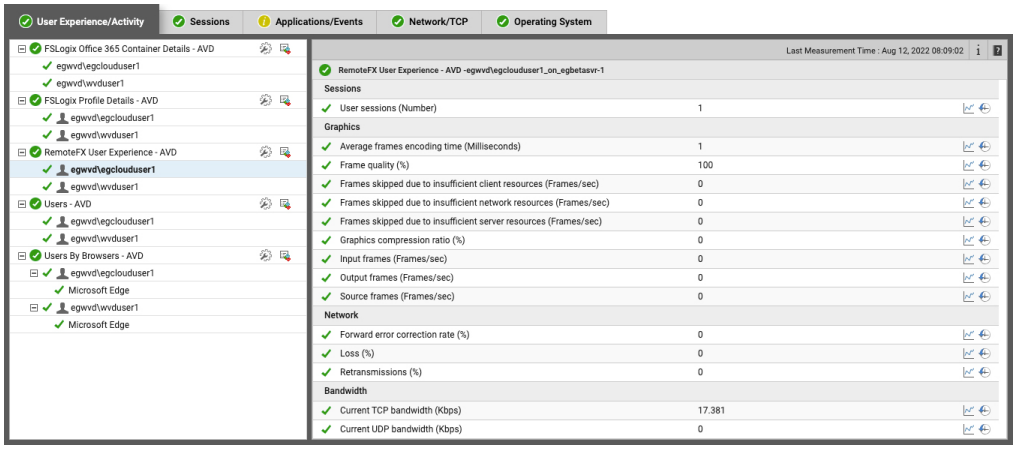


Figure 14: Monitoring of latency and bandwidth used by every AVD session

IT admins can get a quick overview of active user sessions from the User Experience Dashboard. Here, admins get to see a quick overview of all user sessions that are active, and key user experience and resource metrics for each session. They can also drill down into any session and see more details of user activity and performance in that session.

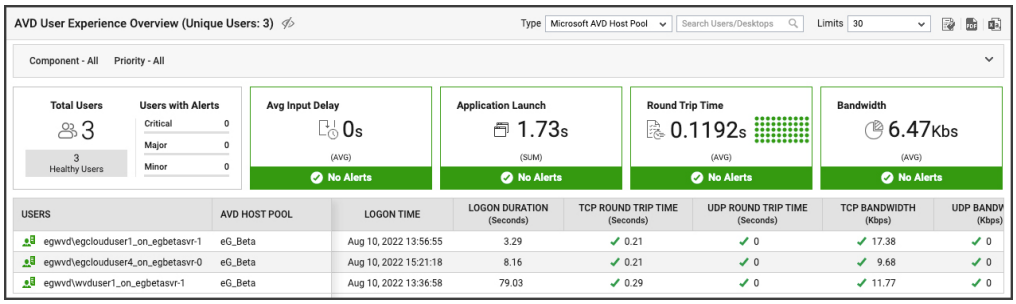


Figure 15: eG Enterprise's user experience dashboard showing all AVD sessions at a glance including details on TCP and UDP latency and performance

Monitoring of AVD Session Hosts

User experience issues can occur if the session hosts have resource bottlenecks, e.g., due to insufficient sizing of CPU/memory/bandwidth/disk resources. eG agents on the session hosts monitor all aspects of the Windows OS performance to identify and resolve OS bottlenecks.

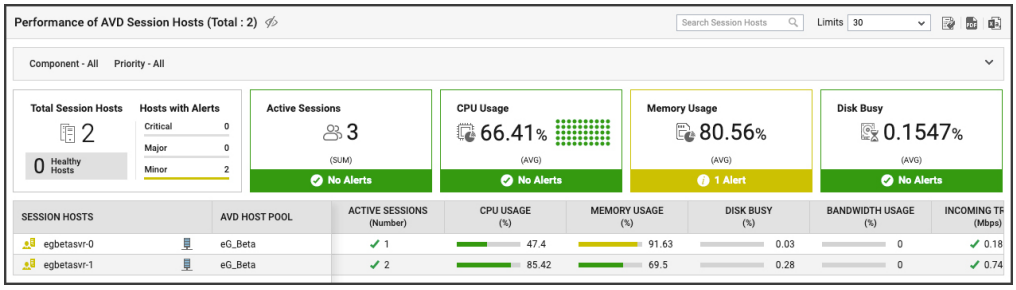


Figure 16: Out of the box dashboards give an overview of the performance and usage of all session hosts

With eG Enterprise:

- Admins can determine if there is a CPU or memory bottleneck and what are the top processes consuming these resources.
- It is simple to differentiate excessive and abnormal resource usage from under-sized resources caused by poor capacity planning
- Disk IOPS and activity are also tracked and the processes causing disk activity are highlighted.
- OS handle leaks can also slow down applications – e.g., if an application keeps opening a file object but doesn't close it. eG agents also detect such conditions and raise alerts pinpointing the applications causing OS handle leaks.
- Network traffic to and from the session hosts is also tracked. Excessive or abnormal bandwidth consumption is highlighted.
- Windows system, security and application event logs are monitored and critical/error events highlighted.

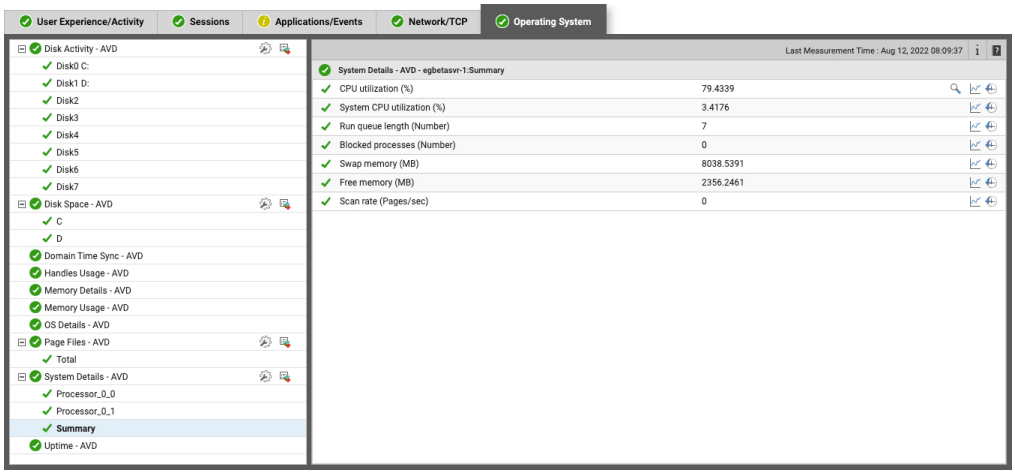


Figure 17: Monitoring of CPU usage on an AVD session host

List of top 10 CPU consuming processes

PID	CPU usage(%)	Application name	ARGS
Jul 11, 2022 11:51:58			
3564	21.09	sapgui	C:\SAP\sapgui.exe
10192	21.09	sapgui	C:\SAP\sapgui.exe
12132	15.63	msedge	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe --type=renderer --disable-client-side-phishing-detectic
6156	1.3	sensendr	C:\Program Files\Windows Defender Advanced Threat Protection\SenseNdr.exe eyJDbGllbnRWZXIiOiIxMC44MDQwLjE5MDQxLjE0MTUiLCJDb21wb25lbnRzIjpbeyJBZGFwdGVySWQiOJ7NTRCQTdEC
3400	1.04	mssense	MsSense
15028	0.52	Console Window Host	\??\C:\Windows\system32\conhost.exe 0x4
2064	0.26	Host Process for Windows Services	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
10672	0.26	Windows Explorer	C:\Windows\Explorer.EXE
12424	0.26	msedge	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe --flag-switches-begin --flag-switches-end
13520	0.26	Console Window Host	\??\C:\Windows\system32\conhost.exe 0x4

Figure 18: Detailed diagnosis shows the processes responsible for the CPU usage of a session host

- Session activity on the hosts is monitored. Session disconnects leave behind running processes even though a user is not active in a session. This can result in resources on the host being wasted. eG Enterprise can detect and alert to such conditions.

- Input delay, which is the delay in processing requests from users, is tracked for every session. High input delay is indicative of bottlenecks on a session host.

- Browser activity on a session host is also monitored. Resources consumed by each user/browser combination are reported and details captured include active URLs. This information can be useful for an IT admin to determine which URLs were active when a browser instance started consuming a lot of resources. Browser specific issues become easy to identify.

In addition, resource usage is tracked for each and every user session on the session host, so if a user does raise a support case or call, the help desk operator or administrator can easily figure out why and oversee the user's individual experience and configuration.

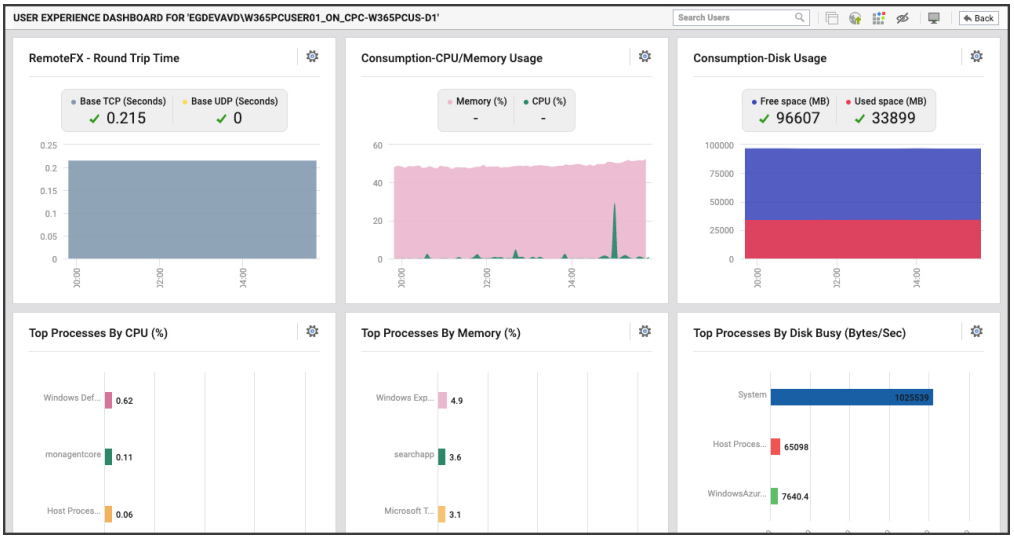


Figure 19: User experience dashboard for a user session highlighting the resource usage over time and the top resource consuming applications

Monitoring of AVD Session Hosts Alone is Not Sufficient

While monitoring of user experience and session hosts is important, it is simply insufficient to monitor and diagnose the performance of the virtual desktop service. The Azure Control Plane is where a lot of decisions are taken on how to process user requests, and therefore, monitoring it is vitally important. Users are authenticated via Azure Active Directory and hence, it is important to track its performance and failures. In a similar vein, the session hosts are configured in an Azure subscription. Hence, the configuration and usage levels have to be tracked in the Azure subscription.

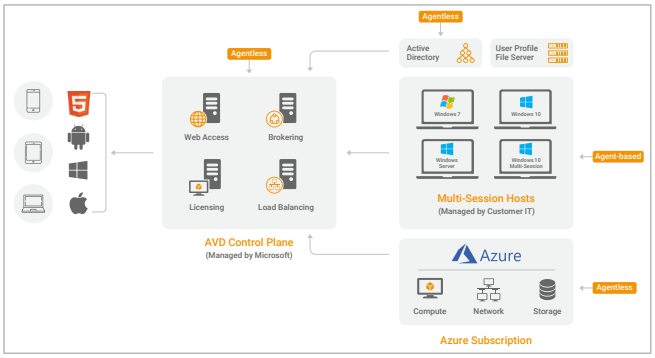


Figure 20: How eG Enterprise monitors every layer and every tier of your AVD deployment

Therefore, to get a complete view of your AVD deployment, it is important to monitor:

- Connection brokering in the Azure Control Plane
- Azure AD availability and performance
- The Azure subscription
- The Azure host pools and their session hosts

While eG Enterprise uses agents on the AVD session hosts, monitoring of the Azure control plane, the Azure subscription and Azure AD is agentless. If you are using a hybrid identity management approach, then you need Azure AD Connect to integrate your on-prem Active Directory and Azure AD. eG Enterprise monitors Azure AD Connect in an agent-based manner.

Monitoring of Azure Connection Brokering

One of the key components of the Azure Control Plane is the Azure Virtual Desktop Connection broker which is responsible for scaling up/down session hosts and for allocating users to the session hosts. For monitoring the AVD broker, eG Enterprise tracks:

- Errors of different types for each host pool: Connection errors, feed errors, management errors, and service errors.
- Connections in different states (e.g., connected, completed, failed, etc.) by host pool
- The health status of all the session hosts – e.g., domain joins, URL checks, healthy hosts, etc.
- Logon performance for users. The complete user logon processing is visible only to the connection broker because it is the one handling all stages of the logon process.

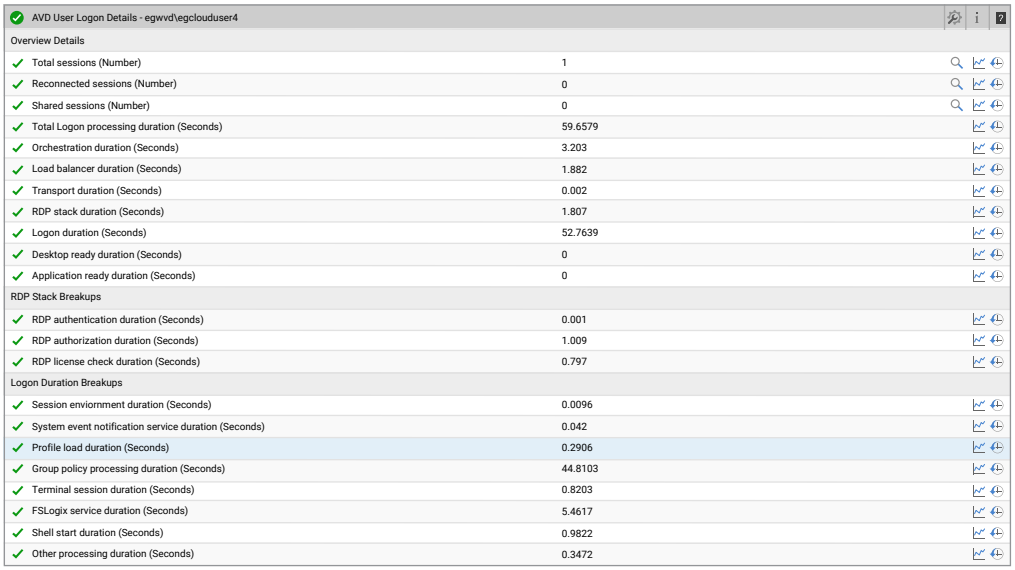


Figure 21: Overview of user logon performance as reported by the AVD connection broker

Monitoring of Azure AD

Monitoring, managing and auditing the entire authentication stack is critical in an AVD deployment to not only ensure users can access their applications and workspaces, but to ensure a secure system where only authorized services and users can access resources and data.

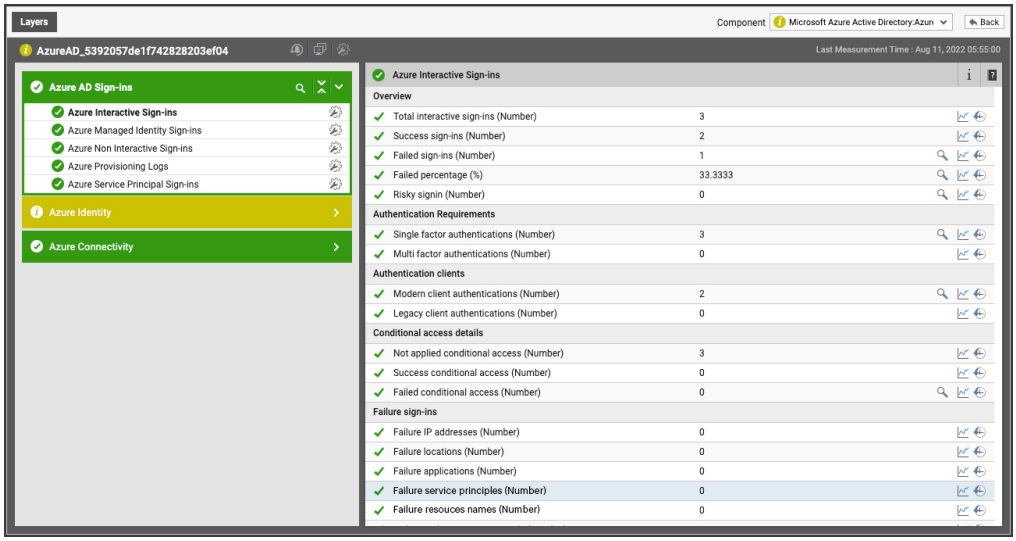


Figure 22: Monitoring model of an Azure AD

Tasks such as checking App Client Certificates are often implemented via PowerShell scripts by administrators. eG Enterprise removes the need to write and maintain custom scripts, thereby improving ITOps efficiency. With eG Enterprise, IT teams can:

- Proactively monitor and be alerted on Azure AD App Client Secret and Certificate expirations
- Identify unassigned directory roles
- Identify users who are inactive or have never signed in
- Track users whose passwords are not expiring
- Audit user updates, password changes, application updates, service principal updates, etc.
- Learn about audit failure activities
- Track different sign-in logs including service principal, interactive, managed identity and non-interactive sign-in logs. Failed sign-ins, conditional access failures, etc. are highlighted.

Monitoring of the Azure Subscription

Session hosts are provisioned in an Azure subscription. Tracking of resource usage levels of the hosts relative to the resources provisioned to them must be done via Azure APIs associated with a subscription. eG Enterprise monitors all key aspects of an Azure subscription. Storage bottlenecks are detected by

monitoring availability, used capacity for files, blobs, tables and queues, ingress and egress traffic from the storage account and latencies for access. Besides native Azure storage, NetApp file volumes and file capacity pools are monitored.

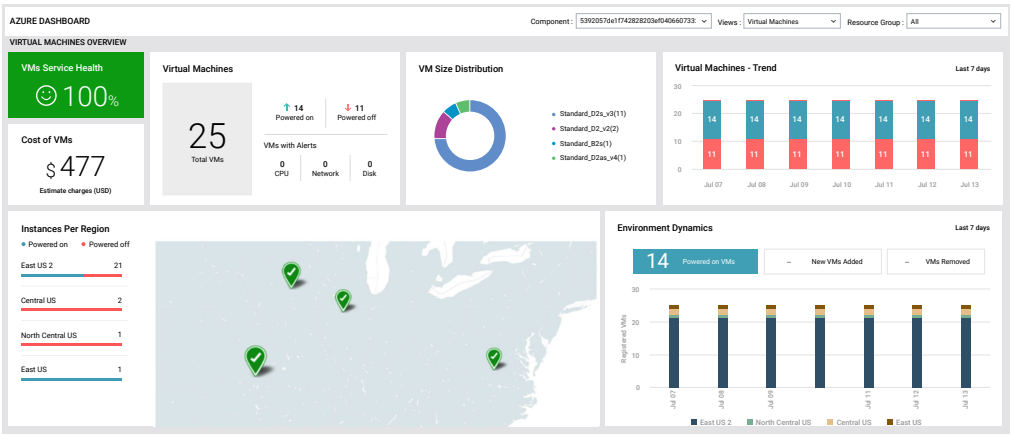


Figure 23: Dashboard showing KPIs for an Azure subscription

For each VM (Virtual Machine), CPU usage, disk IOPS and network traffic are tracked. By comparing these metrics across VMs, IT teams can identify the most resource consuming VMs. eG Enterprise also tracks billing metrics as well as Azure Advisor insights to give a single pane of glass from where IT teams can monitor all aspects of their Azure subscription.

Auto-Discovery and AIOps Capabilities

Auto-discovery capabilities make eG Enterprise simple to provision. Install agents on your session hosts and have your host pools auto-discovered. Alternatively, configure your Azure subscription and the host pools and session hosts are auto-discovered.

eG Enterprise embeds a number of AIOps capabilities to make it easy to monitor, diagnose and report on AVD environments. Any of the metrics collected can be auto-baselined based on time of day, day of month characteristics. Service topology views showing the dependencies between different tiers is used for auto-correlation.

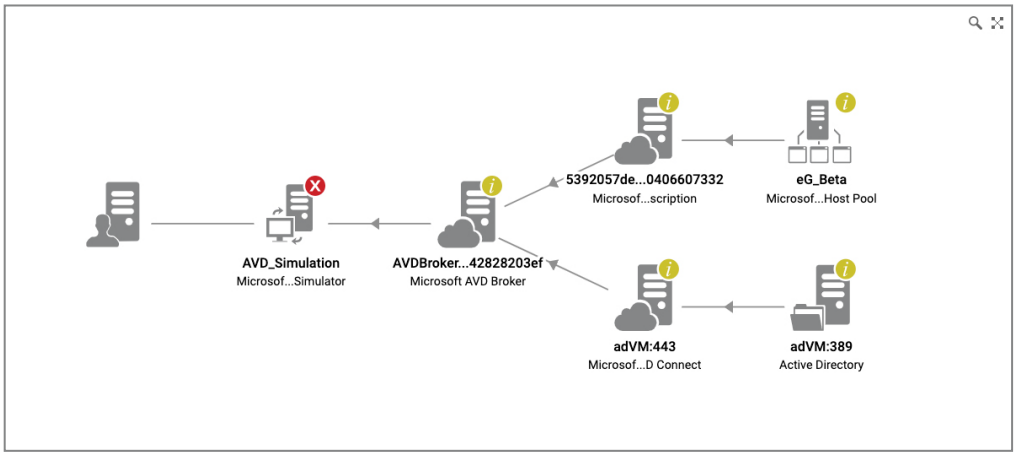


Figure 24: Topology of an AVD service depicting the different tiers involved, their states and the inter-dependencies between them

A number of pre-defined reports are available out of the box with the solution. Without needing to learn any query language or to write scripts, IT admins can quickly access various reports of interest. Common questions like who accessed the AVD environment, when, for how long, what applications did they access, and what resources they used can be answered using built-in reports that are accessible in a few clicks. eG Enterprise reports also assist with post-mortem analysis of problems and can be used for historical reporting and trending as well.

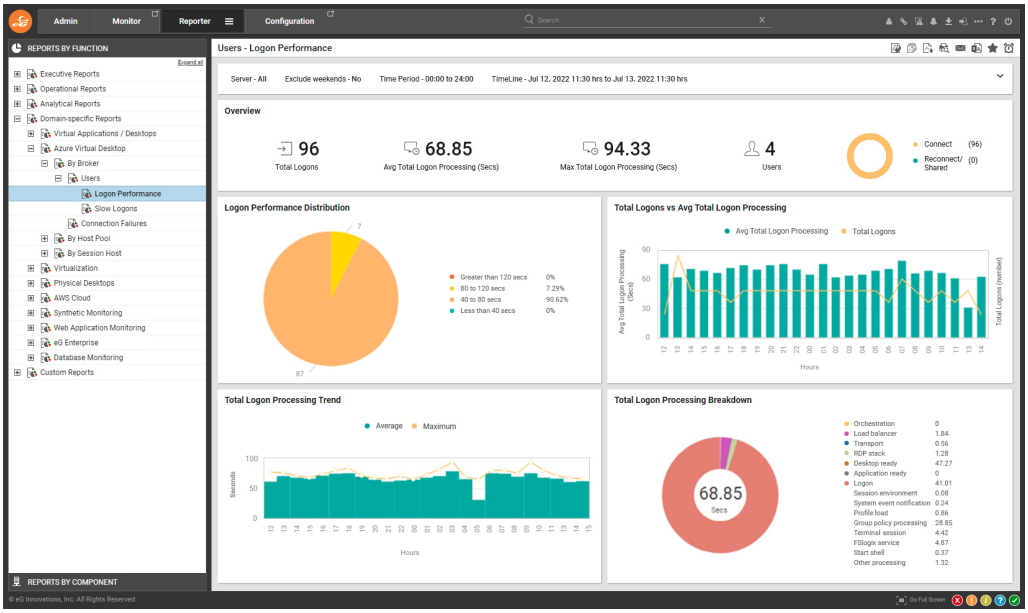


Figure 25: Logon performance reports in eG Enterprise

❖ Conclusion

Widespread adoption of Azure virtual desktop technology is on the horizon. Organizations deploying AVD will need simple and effective ways to monitor AVD. In this blog, we discussed why AVD monitoring requires specialized tools and compared Azure Monitor and eG Enterprise and their capabilities for AVD monitoring, diagnosis and reporting. Details of the specialized AVD monitoring, diagnosis and analytics capabilities of eG Enterprise have also been covered.

❖ Learn More

- Azure Virtual Desktop Monitoring Tools – AVD Monitoring | eG Innovations
- Free AVD logon simulator for Azure Virtual Desktop | eG Innovations

❖ Next Steps

- ✉ | To contact eG Innovations sales team : sales@eginnovations.com
- 🌐 | Get a free trial of eG Enterprise : www.eginnovations.com/FreeTrial
- ✉ | For support queries and feature requests : support@eginnovations.com

❖ About eG Innovations

eG Innovations provides the world's leading enterprise-class performance management solution that enables organizations to reliably deliver mission-critical business services across complex cloud, virtual, and physical IT environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations' award-winning solutions are trusted by the world's most demanding companies to ensure end user productivity, deliver return on transformational IT investments, and keep business services up and running. Customers include Anthem, Humana, Staples, T-Mobile, Cox Communications, eBay, Denver Health, AXA, Aviva, Southern California Edison, Samsung, and many more.
To learn more visit www.eginnovations.com