Service Description

Managed Azure Virtual Desktop
August 2025

transparity

transparity

Contents

transparity

1. Service Overview

The Managed Azure Virtual Desktop service includes support, monitoring and a range of proactive services for Microsoft Azure Virtual Desktop (AVD) based solutions.

2. Service Features

The following is a high-level overview of the functionality available within this service:

KEY:

● Inclusive as part of the standard service offering

◒ Inclusive and as standard when you have purchased the relevant service or if you have requested service(s) that have been documented in your SoW.

○ Available as an optional upgrade for an additional fee.

Feature	Advanced
24*7 Incident Response	●
Proactive Monitoring	●
Profile Support	●
Host Patching	●
Gold Image Management	●
AVD environment configuration and management	●
Service Requests	●

2.1 24*7 Incident Response

For Incidents within your Microsoft AVD environment, we will provide 24*7 incident response, if the Incident relates to the services provided by the Microsoft, we will escalate to Microsoft.

We will follow the Target Response as defined in section 8.1 of this service description.

2.2 Proactive Monitoring

As part of this service, we provide proactive monitoring for Azure Virtual desktop services using our monitoring platform.

We will monitor your infrastructure based on best-practice and our expertise.

Full details of the services monitored are available on request.

2.3 Profile Support

We will respond to, investigate, and resolve incidents regarding user profiles where they are raised by our monitoring platform or your IT team.

2.4 Host Patching

We include patching of persistent or personal hosts in your AVD environment only if these host(s) are not rebuilt from the Gold Image when rebooted or powered on. If your hosts fulfil these criteria, we include them in the OS patching schedule for your Azure Advanced Managed Service.

Commented [TM1]: Need to develop a separate monitoring config for this as it causes alot of noise if auto-scaling is turned on.

Commented [RG2R1]: I suspect the information Nerdio surfaces will help here, but yes we need to define what will be monitored.

Commented [AC3R1]: Agreed, We will need to create monitoring and alerting via Azure Native Monitoring or Nerdio. I'm yet to see the Nerdio monitoring capabilities and understand how this would feed into our current ITSM system. Something to consider before we go live.

Commented [TM4]: Might need @Anthony Cooke to confirm this but I believe best practice is to not patch the hosts via normal methods and to re-deploy them via gold image each month as this can cause mis-matches in patch levels between servers, however we have had customers where Windows Auto-Update has been left on and its worked fine.

We will also investigate and remediate OS patches where they fail to install.

2.5 Gold Image Management

We will maintain the Gold Images documented in your Statement of Work. As part of that maintenance, we will: -

- Make minor OS changes, including but not limited to:
  - registry key changes,
  - file/folder creation, and
  - copied files we deem necessary to maintain or improve remote session stability;
- Install OS updates/patching excluding major version updates;
- If applicable for you:
  - install Microsoft 365 desktop application updates/patching, including major version updates;
  - install Microsoft Teams updates/patching, including major version updates;
  - install Adobe Acrobat Reader updates/patching, including major version updates;
  - install Google Chrome updates/patching, including major version updates;
- Deploy to a Validation Environment and test;
- Deploy to a Validation Environment prior to production if available; and
- Deploy to the production group after testing/validation.

Gold Image maintenance will be performed on a monthly basis. All changes (apart from operating system and Microsoft Office minor updates) will be agreed with you in writing via your SDM prior to us performing the maintenance.

New Gold Image(s)

If a New Gold Images is required this would be a chargeable professional services engagement and can be requested as part of this service, creation of additional images will result in an increase to our fee to you for the Service. New images created after the Service Commencement Date will need to be documented in a Statement of Work. Gold Image(s) no longer required by you will be removed from the service and, unless replaced by a New Gold image, our fee for the Service will reduce accordingly.

When creating new gold images, we will: -

- Deploy the Windows version you specify to us;
- Make minor OS changes including but not limited to:
  - registry key changes,
  - file/folder creation, and
  - copied files we deem necessary to maintain or improve remote session stability;
- Install OS updates/patching;
- If applicable to you:
  - install Microsoft 365 desktop applications you specify to us;
  - install Microsoft Teams desktop application;
  - install Adobe Acrobat Reader desktop application;
  - install Google Chrome desktop application;
- Deploy to a non-production group and test; and
- Deploy to a new production group after testing.

Gold Image(s) Testing

For application installation/updates and OS changes you require that are not included in our maintenance or creation activities listed above, we will agree a time window with you whereby the Gold Image will be available for you to connect to and install/update software and make changes. Once that window is complete, we will seal the gold image and test it for you.

Commented [AC5]: Maybe worth noting that if AVD is managed by Nerdio and they are using Golad images then patching would be covered as per the below.

Commented [RG6R5]: @Anthony Cooke I wouldn't call out Nerdio as the tooling in the SD. Might need a hand to understand exactly what to put here.

Commented [AC7]: The customer will need to be available to test this

Commented [RG8R7]: Yes, this is covered in the general obligations about the customer being available to test or support anything where their involvement is required.

Commented [TM9]: Is the desk delivering this?

Commented [RG10R9]: TBC @Anthony Cooke could this be a scheduled monthly PS activity?

Commented [AC11R9]: This would have to be PS but Nerdio should be doing all of this for us anyway. But, What if we have to update an image with settings that resolves an issue that was first logged by the desk. It might be worth adding that to the list of bullets above. E.g. Any configuration chnages required to resolve a ongoing issue.

Commented [AC12]: Are we saying that we wont make gold images for LOB or 3rd party apps as part of the service and that would be a project as it typically is now.

Commented [RG13R12]: @Anthony Cooke no new image builds would be a chargeable PS engagement. I'll clear up the language to sort that out.

Image testing is performed in one of two ways:

- Gold Image Creation –
  - By deploying to an isolated host group to ensure the desktop/apps load and close without crashing.
  - At least two (2) sessions will be started concurrently to ensure multi-session capability isn't degraded. Following this initial testing listed above and its successful pass, we will deploy to a new production host pool.
- Gold Image Maintenance –
  - By deploying to an isolated host group to ensure the desktop/apps load and close without crashing.
  - At least two (2) sessions will be started concurrently to ensure multi-session capability isn't degraded.
  - Following this initial testing listed above and its successful completion, we will deploy to a Validation Environment if one is available to monitor user testing before rolling the updated/new image to a production host pool.

2.6 AVD Environment Configuration and Management

As part of the Service we will monitor, manage, and maintain the configuration of the following aspects of your AVD environment: -

- Host Pools,
- Application Groups,
- Workspaces,
- Scaling Plans,
- AVD Users and user sessions,
- Custom Image Templates – these will be your gold images, and
- FSLogix User Profile Containers.

We will do the above as necessary to deliver our obligations as part of the Service and maintain availability of your AVD environment for you.

Commented [AC14]: I assume we wouldn't be adding new Host pools and groups as part of this? For example if a customer decided they now want the HR department to use AVD and have their specific apps added?

Commented [RG15R14]: @Anthony Cooke correct, that would be a PS engagement to build a new gold image with the appropriate apps.

2.7 Service Requests

The managed service includes a defined number of service requests per month based on your AVD consumption, the number of service requests included with your service will be detailed in the statement of work at the point of order.

3. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

4. Billing

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

- Implementation work carried out outside Business Hours; and
- Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the service subject to the following dependencies:

- All professional services required to set up this Service will be subject to separate Statements of Work and Charges and, where applicable, Service Descriptions.

5.1 Customer Obligations

- You will provide us reasonable assistance in the performance of the Service(s) including, but not limited to, providing all technical and licence information that we may require to perform the Service(s).
- You will provide named contacts who will be authorised to submit support requests on behalf of your company ("Nominated Contacts"). They will be the designated people with whom all contact is made regarding all requests.
- You will provide us with access to the in-scope subscriptions, accounts, and tenants. This access will be used by our support staff and tooling. For example:
  - Microsoft's Partner Admin Link (PAL);
  - Microsoft Granular Delegated Access Permissions (GDAP) relationship;
  - Azure Lighthouse relationship and delegations;
  - Service Principals;
  - Administration break-glass accounts; and
- For Azure subscriptions not purchased through our CSP we will not be able to raise incidents with Microsoft unless you have purchased a separate Microsoft support agreement;
- You will allow us to deploy infrastructure in each public cloud region to handle the collection of activity and diagnostics logs into our monitoring platform.
- You are responsible for having an associated licence (where legally required or contractually required by the vendor to do so) for:
  - Operating System(s) (OS) and software for your applicable Public Cloud Resources.
- You will provide us with reasonable advance notice of any:
  - intent to perform planned maintenance activities (including upgrades, deployments, patching);
  - additional resources that you will deploy into the Supported Public Cloud Platform.
- You will actively work with our operations team to resolve any raised incidents or Service Requests, or any activities relating to patching, that require your input or action. For example, you may be required to make any required changes to an OS running within a VM to which we have no access.
- Some incidents may require user-impacting remediation activity. You are responsible for distributing and coordinating end-user communications and activity unless agreed otherwise during the planning of the activity.
- It is your responsibility to comply with your data sovereignty controls, policies, and procedures.

5.2 Service Restrictions

- We will provide and support the Service on a reasonable endeavours basis only and will not be subject to any availability targets, if:
  - the OS residing on your VM resources is out of vendor support, or
  - no support contract with the OS provider is in place, or
  - the Supported Public Cloud Environment and or resources are configured in direct contravention of the requirements, best practices, or specific guidelines for support.
- When a ticket is opened with a Public Cloud Vendor the Transparity SLA is paused until a response is received from the respective Public Cloud Vendor

- PaaS monitoring is for the Microsoft Azure PaaS service and supporting Microsoft Azure infrastructure only. We will not monitor the applications or custom configuration that is deployed to these services.

6. Exclusions

6.1 Third Party Related

- Managing incident maintenance for:
  - 3rd party systems,
  - Software, and/or
  - SaaS services
- Specifically, if the above items are not covered by a third party's warranty, support agreement, or terms of use.
- We do not support any service(s) purchased from a Public Cloud Vendor marketplace.
- We do not guarantee the availability, capacity, or performance of the Supported Public Cloud Platform;
- We do not monitor, support, or assure the integrity, functionality, or availability of pipelines, code, applications, or any other processes within your Supported Public Cloud Platform.
- Any software or data deployed, installed, consumed, developed, operated, or generated in the Supported Public Cloud Platform is excluded from this Service;
- Microsoft Entra ID (formerly known as Azure Active Directory) or Microsoft Windows Active Directory either in your Supported Public Cloud Platform or any other location is excluded from this Service;
- Updates to client devices and software are out of scope unless otherwise agreed;
- Certificate management is limited to server endpoints and platform services. Certificate renewals or management on end user devices is not in scope.

7. Definitions and Acronyms

In this document "we" or "us" refers to the Supplier, and "you" refers to the Client.

7.1 Terms

The terms listed have the following meanings:

Term	Meaning
Statement of Work	This means a document that defines project-specific or Customer-specific activities, deliverables, and/or timelines for providing services to that Customer.

7.2 Acronyms

Acronym	Meaning
CSP	Cloud Solution provider
GDAP	Granular Delegated Access Permissions
OS	Operating System
PAL	Partner Admin Link
PaaS	Platform as a Service
SLA	Service Level Agreement

Acronym	Meaning
SSL	Secure Sockets Layer
SoW	Statement of Work
VM	Virtual Machine
VPN	Virtual Private Network
WAR	Well Architected Review

8. Service Level Agreement and Operational Targets

8.1 24*7 Incident Response

	P1	P2	P3	P4
Hours of Support	24*7 Monday – Sunday	24*7 Monday – Sunday	08:00-18:00 Monday – Friday	08:00-18:00 Monday - Friday
Response	15 mins	Four (4) hours	Eight (8) hours	Twelve (12) hours

8.2 Incident Prioritisation

Priority	Severity	Description
P1	Critical	**Business service outage** • System/Service/Application down or unhealthy. Extremely urgent • Very high impact in all business areas, extreme impact on multiple users and disruption is excessive, such as Cloud platform failures, Virtual Machine failures and Cloud networking or connectivity failure • Business critical - work cannot continue
P2	High	**Business service impaired** • High impact on significant business areas or specific users • Individual user cannot complete high priority/business-critical work, or department or group of users unable to continue with routine work • Business-critical work is impaired
P3	Medium	**Group of users affected** • Platform or application problem – user or group priority work cannot be completed • A group of users are experiencing system or business application
P4	Low	**One (1) person affected or minor service fault** • Minor system or application error • Backup or Patching Failure • An individual user is experiencing system or business application problems but is still able to work
P5	Routine	**Non-urgent investigations** • General advice and guidance or agreed scheduled activity