Business

Technical appendix to the Managed Applications Service Description
Managed OS

Table des matières

1 Definitions

In addition to the definitions of the General Terms and Specific Terms for Integration, Maintenance, and Associated Services, the following specific definitions apply to this Service Description.

Environment refers to a private virtual resource space on the IaaS that can only be accessed by Users authenticated via login and password. Actions such as creation, destruction, modification, and listing of these resources and associated functionalities are limited to these Users only.

Client Administration Environment refers to the environment where the Client's Service (build and deployment) is hosted. Actions such as creation, destruction, modification, and listing of resources and associated functionalities are limited to the Provider.

Client Environment refers to the environment where the Client's containers are deployed. Actions such as creation, destruction, modification, and listing of resources and associated functionalities are assigned to both the Provider and the Client. The Client can use this tenant to run applications and utilize IaaS.

RACI refers to the definition of responsibilities between the Client and the Provider. R = Responsible, A = Accountable, C = Consulted, I = Informed.

Tenant refers to a private virtual resource space on the IaaS that can only be accessed by Users authenticated via login and password. Actions such as creation, destruction, modification, and listing of these resources and associated functionalities are limited to these Users only. For IaaS using VMware technology, the Tenant is also referred to as "Organization."

Managed Tenant refers to the Tenant where the Client's Service is hosted. Actions such as creation, destruction, modification, and listing of resources and associated functionalities are limited to the Provider.

Token refers to the unit of work used to express the prices applicable to changes requested by the Client, as indicated in the Pricing Sheet.

2 Object

This service description aims to define the conditions under which the Provider delivers the "Managed OS" service (hereinafter referred to as the "Service") to the Client.
This description is linked to the document "Managed Applications – Service Description."

3 Service Presentation

3.1 Service overview

The managed OS service provides administration, monitoring, patching, and security for Linux and Windows operating systems hosted on Cloud Avenue, vCoD, or any other infrastructure.

As part of the Managed OS service, we also provide complete management of the operating system of a VM (Virtual Machine) hosted on the Public Cloud IaaS infrastructure from the list below:

- Cloud Avenue (the Provider)
- Flexible Engine (the Provider)
- AWS (Partner)
- Microsoft Azure (Partner)
- Google Cloud (Partner)

We also provide complete management of the operating system of a physical server hosted exclusively on the Provider's IaaS (Cloud Avenue and Flexible Engine).

We operate during the following two phases:

- Commissioning
- Operational Maintenance

The list of supported operating systems:

OS	Distribution and version
Linux	- RedHat Enterprise - CentOS - Ubuntu - Debian
Windows	- Windows Server

The customer is responsible for application and middleware management and for verifying its working condition.

4 Prerequisites

4.1 Secured Bastion

The Bastion service is a prerequisite for all Managed Applications services, including Managed OS.
The use of Bastion MASERPAM is mandatory for all privileged access within the Managed OS service.

4.1.1 Bastion (MASERPAM)

Mandatory use of the MASERPAM Bastion.

A bastion is a security solution that protects access to privileged accounts within an information system in order to administer hosted services.

MASERPAM Bastion is a security solution that protects access to privileged accounts in an information system. Based on CyberArk Alero/Remote Access, it relies on a secure vault where sensitive identifiers, secrets, certificates, and keys are stored and encrypted. Each access is temporary, tracked, and recorded to ensure security, compliance, and accountability.

The use of Bastion MASERPAM is a mandatory prerequisite for all Managed Applications services (Managed OS, Managed Database, Managed Middleware, Managed Applications), regardless of the hosting environment (Cloud Avenue, vCoD, or other infrastructure).

This system guarantees the security, confidentiality, and traceability of privileged access, in accordance with compliance requirements (HDS, PSSI, PGSSI-S) and service quality commitments.

Direct access to managed resources without going through the Bastion is strictly prohibited.

For services falling within the scope of IaaS/vCoD console (CAV), the use of the MASERPAM Bastion is not currently required by contract but remains strongly recommended, particularly for user accounts with administrative privileges.

The user authenticates with the bastion and obtains temporary access to the requested resources. Access is monitored and logged, allowing the user's actions to be tracked.

In summary, a bastion is a security solution that reduces the risk of privileged accounts being compromised and strengthens the overall security of the information system.

4.1.2 Service Overview

As part of Cloud projects hosted on the Cloud Avenue platform, the Provider implements a secure Bastion for Clients requiring privileged access for the administration of their information system.
The use of a Bastion is a prerequisite:

- To meet cybersecurity requirements,
- To maintain confidentiality and protection of privileged access data,
- To ensure the quality-of-service commitments, particularly by tracking the actions of various stakeholders involved in the system

The Provider mandates the use of an administration Bastion to perform all actions on the services we operate.

The Provider is fully and exclusively responsible for managing the administration Bastion, which provides:

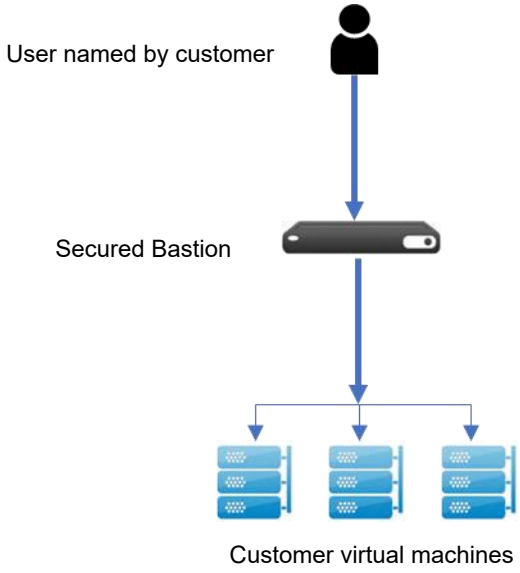
- Centralized access to the platform/service,
- User management,
- Privilege management,
- Secret management,
- Traceability of actions performed through the bastion.

4.1.3 Key features

- Strong biometric authentication via CyberArk Alero
- VPN-free access via secure web interface (RDP, SSH)
- HTTPS option with dedicated connector (specific OTC)
- Centralized management of credentials, secrets, and certificates (Vault)
- Complete logging and video recording of sessions (viewable only by BSO)
- Automatic rotation of passwords and access keys

4.1.4 Functional Diagram of the Solution

Ce schéma d'architecture fonctionnelle illustre comment le Bastion sécurisé est utilisé pour protéger l'accès à des machines virtuelles, en fournissant une couche de contrôle et de sécurité supplémentaire pour les utilisateurs nommés.



4.1.5 Units of Work (UO) and Pricing

The pricing for the Secure Bastion Service is composed as follows:

- A mandatory UO for Clients who have subscribed to a Managed Tenant – small, covering the bastion service foundation. The bastion service foundation is included in the Managed Tenant – medium and large subscriptions.
- A mandatory UO with an OTC/MRC price for 2 named users of the Client for access to the Client's resources (VMs, Applications) via the secure Bastion. This UO covers the Bastion service and the necessary licenses for 2 named users.
- An optional UO with an OTC/MRC price per additional named user of the Client for access to the Client's resources (VMs, Applications) via the secure Bastion. This UO covers the Bastion service and the necessary licenses for 1 named user.

5 Included Services

As part of the Managed OS service, we manage infrastructure components. Some services are included with the Managed OS, while others are offered as options.

5.1.1 Antivirus

As part of the Managed OS service provided for a VM or physical server hosted on a Cloud infrastructure, we deploy Trend Micro Deep Security antivirus and manage updates, configuration, and monitoring.

This antivirus scans and detects viruses, spyware, and Trojans in real-time (during file access). In the event of a virus detection, the item is automatically quarantined for analysis or deleted if the first action is not possible.

5.1.2 Vulnerability Scan

As part of the Managed Service, the Provider conducts regular vulnerability scans to ensure the security of the assets for which it is responsible. This service allows the Client to maintain the recommended security level and effectively mitigate risks. Vulnerability corrections are handled by the Provider's teams within the scope of the service subscribed by the Client (Managed OS, Managed DB, or Managed Application).

The Provider uses security tools to assess the network, applications, and infrastructure for weaknesses that could be exploited by malicious actors.

A detailed report by tenant is made available quarterly in the Client space, describing the top 10 identified vulnerabilities and recommended remediation steps under the Client's responsibility.

At the Client's instruction, the remediations under their responsibility can be addressed and may result in a quote from the Provider to the Client.

5.1.3 Backup

To ensure service recovery in case of issues, we recommend at least a Snapshot backup with a 6-day retention period. Backups are performed during off-peak hours, and the backup operation is ensured according to the level of support subscribed.

A different retention period may be chosen based on the availability of the backup from the Cloud infrastructure hosting the service.

5.1.4 Monitoring

We provide the following monitoring for the VMs or physical servers we manage. The table below presents the type of monitoring and associated actions.

Type	Monitoring	Action
Manual	Monitoring System Files (Linux Repositories, etc.)	In case of malfunction, the operations team is notified via a ticket to resolve the issue during business hours.
Automated	Monitoring OS Obsolescence	In the event of obsolescence, you will be notified, and the sales team will initiate an update project.
Automated	Monitoring Updates for Agents and Reporting Databases (Antivirus/Security Patches)	In case of malfunction, the operations team is notified via a ticket to resolve the issue during business hours.
Automated	Monitoring OS Availability	In case of an alert (OS down), the operations team is notified via a ticket to resolve the issue during business hours.
Automated	Monitoring OS Performance	In case of a performance alert (based on a defined threshold), the operations team is notified via a ticket to resolve the issue during business hours.
Automated	Monitoring for viral presence and containment	In case of an alert, the operations team is notified via a ticket to resolve the issue during business hours. Actions will need to be approved with you.

5.1.5 Log management

On Cloud Avenue, a centralized log management service is offered and is structured as follows:

- Log Collection: The service automatically collects logs generated from Managed OS and security components subscribed by the Client.
- Log Storage: The collected logs are securely and durably stored in a centralized location. The Provider offers a standard retention period; other retention durations may be subject to a specific proposal from the Provider to the Client.
- Log Usage: The logs are for internal use by the Provider's administration teams.
- Log Provisioning: Upon request for change, the Provider will perform an export of the logs for the Client.

5.1.6 Reporting - Option

We offer two levels of reporting

- Usage: Reports on infrastructure status, service health, capacity, performance, and consumption.
- ITSM: Reports on change management, incident management, and SLAs.

5.1.6.1 *Usage*

Usage reports present the status of your managed Cloud infrastructure over a selected time frame. These reports are accessible from the Cloud Client Space.

The available indicators are:

Ressource	Indicators
Server (VM or physical)	- Server Availability - CPU Usage - Number of Processes - Memory Usage - SWAP Space Usage - File System Usage - Bandwidth Usage

	- Server Status (Off, Standby, Active)

5.1.6.2 *ITSM*

ITSM reports present the status of managed services over a selected time frame. These reports are accessible from the Cloud Client Space.

Service availability	
Service	**Indicators**
Nom su service	- Number of incidents during the selected period classified by priority level (P1, P2, P3, P4) - Resolution time for each incident - List of incidents where the GTR commitment is not met - List of incidents where the GTI commitment is not met - List of incidents by status (open, acknowledged, in progress, resolved, etc.) - Monthly evolution over 1 year.

Incidents	
Service	**Indicators**
Nom du service	- Contractual GTD Commitment (Guaranteed Availability Rate) - Measured GTD - Monthly evolution over 1 year.

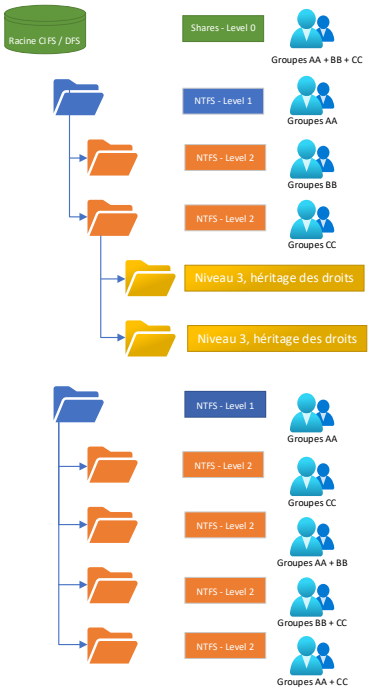
Change requests	
Service	**Indicators**
Nom du service	- Number of requests during the selected period classified by type - Processing time for each request - List of requests where the GTT commitment (Guaranteed Processing Time) is not met - List of requests by status (open, acknowledged, in progress, processed, etc.) - Monthly evolution over 1 year - Consumption of tokens from the package

6 Optional services

6.1 Managed Filer

With this service, depending on the chosen technical solution, we manage files to meet the client's data storage and sharing needs. We handle the configuration, monitoring, and maintenance of your file system, allowing you to focus on your core business. Our service includes access permission management, regular data backups, storage capacity management, and technical issue resolution.

The Managed Filer includes the implementation of access security on Shares and the NTFS file system for the first two levels of the distributed file system hierarchy (CIFS, DFS & DFS-R). The implementation of hierarchy security will be carried out using Active Directory groups pre-filled by the client and communicated to the Provider's operations team in advance.



7 Price conditions

7.1 Price

The pricing for the Managed OS Service is composed of:

- Access fees for the "Managed OS" service, which include all tasks mentioned in the implementation RACI and are indexed to the number of servers and features to be configured.
- A monthly recurring fee covering activities related to maintaining the operational condition of the infrastructure foundation and the "Managed OS" service, indexed to the number of servers.
- License costs.

The service rates do not include:

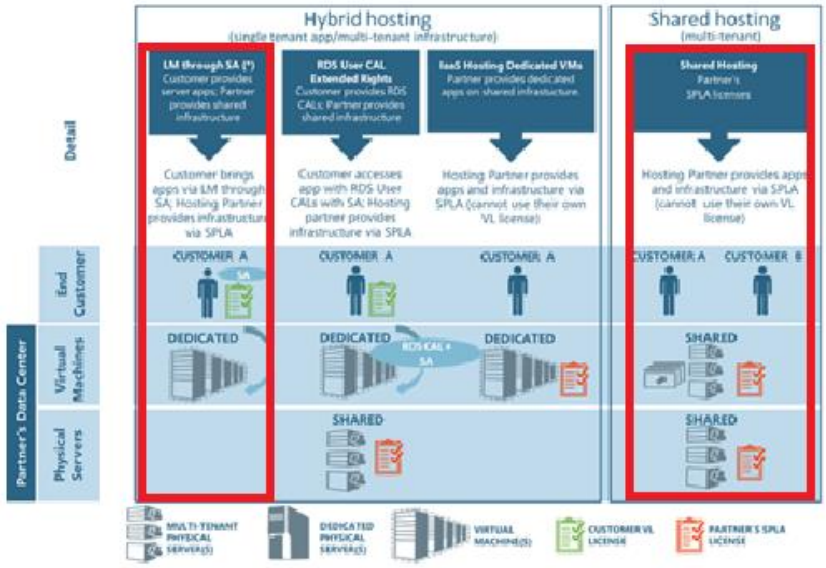
- The cost of the infrastructure that you must subscribe to separately from the IaaS provider at the prevailing rates.
- Change requests.
- License costs.

For the "Managed Filer" option, the pricing is composed of:

- Setup fees that include all implementation tasks and are indexed to the number of filers.
- A monthly recurring fee covering activities related to maintaining the operational condition of the filer, indexed to the reserved volume (in GB).

7.2 Licensing

The client has 2 options for contracting licenses, as illustrated in the diagram below:



1. BYOL (Bring Your Own License): Provide your own licenses (License Mobility through SA, hybrid hosting). In this mode, the client must subscribe to the mobility program and have active Software Assurance.
2. Purchase licenses from the Provider as part of their SPLA (Shared Hosting Multitenant) contract.

8 Service access

8.1 Prerequisites

The "Managed OS" service relies on an IaaS service, which you must also subscribe to. In this context, we manage the Tenant and associated resources.

For systems in an Active Directory, we require an Administrator-type account to perform our Managed OS tasks, granting us access to the file system, registry configuration, system configuration, and deployment of our tools (monitoring, backup/restoration, patch management, remediation).

For Linux systems (CentOS, RHEL), we need an equivalent Root/Sudoer account on the machines covered by the Managed OS. This account is necessary to run Ansible Pipelines and deploy patches.

8.2 Implementation

We perform the following tasks to set up the service on a server:

ID	Tasks	Provider	Customer
Tenant			
1	Grant access to the tenant		A
2	Define policies related to operating systems, procedures, and system services.	A – R	V
3	Define the technical configuration of operating systems in accordance with the requested services (version, languages, file system configuration, system parameters, etc.).	R	A – R
4	Configure the tenant on the chosen IaaS	A - R	
5	Standardize the OS in the case of life and shift	A - R	
6	Configure the service zone to deliver all services	A - R	
7	Provide Customer access to services (cloud customer space, ITSM)	A - R	I - V
8	Provide the elements required for server commissioning using an SRF (service request form)	V	A
9	Install operating systems on servers.	A – R	V
10	Configure services: OS, monitoring, standard backup, antivirus.	A - R	V
11	Define performance indicators for hardware and operating systems, including thresholds and quotas.	A – R	R
12	Develop and document control procedures in accordance with the subscribed service.	A - R	I
R: Responsible – A : Accountable – C : Consulted – I : Informed – V : Approval			

8.3 Operational Maintenance

We ensure operations for maintaining the operational condition of the OS.

The measures taken to achieve this objective can be either preventive or corrective.

The table below presents the tasks and responsibilities associated with the operation of the services outlined in §3.

ID	Task	Provider	Customer
1	Operate the monitoring system.	A – R	
2	Process alerts and incidents and escalate as described in the procedures.	A – R	
3	Implement preventive measures for proactive monitoring and self-healing features to minimize outages affecting service delivery.	A – R	
4	Resolve system incidents in accordance with the service level agreement.	A – R	I
5	Monitor thresholds and occupancy rates and take necessary actions in case of exceedance.	A - R	R – V
6	Monitor the proper functioning of system components according to defined thresholds.	A – R	
7	Monitor performance trends and resource consumption to anticipate potential issues.	A – R	I
8	Generate reports on events upon request and in accordance with the change management process.	A – R	V
9	Advise on appropriate hardware for new configurations or improvements to existing configurations to meet subscribed service levels.	A – R	C
10	Administer and maintain hardware configurations and operating system settings, parameters, and system resource files.	A – R	
11	Manage software license files for operating systems and user keys.	A – R	C
12	Perform corrective maintenance on hardware and operating systems: patch management, intervention management.	A – R	
13	Update and monitor configuration parameters for hardware and operating systems: processor, memory, storage systems, disk quotas, user profiles, etc.	A – R	V
14	Analyze operating system logs.	A – R	
15	Monitor performance indicators for hardware and operating systems, including thresholds and quotas.	A – R	
16	Detect and analyze any abnormal conditions of hardware and operating systems, and take necessary corrective actions.	A – R	
17	Apply changes in accordance with the change management process.	A – R	R
18	Conduct proactive trend analyses to identify recurring issues.	A – R	C – I
19	Track and report any recurring issues or outages and provide a list of consequences related to problems impacting the Client's business.	A – R	I
20	Recommend solutions to resolve any recurring issues or outages.	A – R	C
R: Responsible – A : Accountable – C : Consulted – I : Informed – V : Approval			

9 Support

Below is the specific support we provide for the Managed OS.

9.1 Patch management

Patches provided by the operating system vendor are applied once a month. The OS is fully backed up before applying a patch.

To reduce risk to the service and allow the client to measure the impact of a patch, they can divide their OS service units into 2 groups: "Group 1 Patch" and "Group 2 Patch."

The Provider informs the client of the week and day when the patch is applied for the "Group 1 Patch": from Monday to Thursday of the first, second, third, or fourth week. The patch for "Group 2 Patch" is always applied the week following "Group 1 Patch."

Patches are deployed automatically using specialized tools outside of working hours during the chosen time slot. Any potential failures are then corrected during working hours.

If our monitoring detects an error after applying a patch, the operations team opens an incident ticket and addresses it with the possibility of restoring from the last OS backup if necessary.

9.2 Change management

Change management for the Managed OS service is part of the common model for our managed services. You have access to a catalog of standard requests presented in Chapter 8.

For out-of-catalog requests, the operations team assesses their feasibility. Two scenarios may arise:

1. **Easily Qualifiable Request:**

The operations team will inform you of the number of Tokens required for execution and, if applicable, the necessary infrastructure resources and resulting recurring service load. Upon your agreement, the request will be executed. You will be billed for:

- The number of Tokens deducted from your package if you have subscribed to one or outside the package.
- Additional infrastructure resources according to your Cloud infrastructure contract.
- The recurring service load.

2. **Specific Qualification Request:**

The operations team will inform you to contact your sales representative.

Appendix 1 – Catalogue of standard requests

Catalogue	Category	Description	Number of tokens
Managed Services : OS	OS	Create/extend/delete a Filesystem	1
		Install a component (patch, tool, prerequestite)	2
		Configure the OS (kernel, groups, users, sudo)	2
		Request temporary administrator rights for 48 hours	3
		Start/stop a process	1
		Start/stop a server	1
		Other requests	3
		Add a managed OS	6
		Remove a managed OS	1
		Modify antivirus configuration	2
Managed Services : Infra	Infrastructure	Request an IaaS change	2
		Modify resources of a managed OS (CPU, RAM, Storage, Network)	2
Managed Services : Common	Non-Standard	Request a quote for a non-standard change	
		Accept the price proposal for a non-standard change	
	DNS	Add an entry	1
		Modify an entry	2
		Delete an entry	1
		Others	3
	Communication	Request information	2
		Provide information to the provider	
	Certificate	Install a provided certificate	2
		Regenerate a certificate key	2
		Delete a certificate	2
	Backup	Request a backup or restore	2
		Update the backup policy	2
		Occasional backup	1
		Modify backup parameters	1
		Restore data	3
		Data restoration testing	3
	Service	Delete a managed service unit	2
		Create a managed service unit	3
	Vulnérability	Request explanation and recommendation for a vulnerability	1
		Request a tenant scan	
Optional services			
Managed Filer		Create quota	2
		Increase quota	2
		Create share	2
		Delete share	2
		NTFS security up to 2 levels: share	5