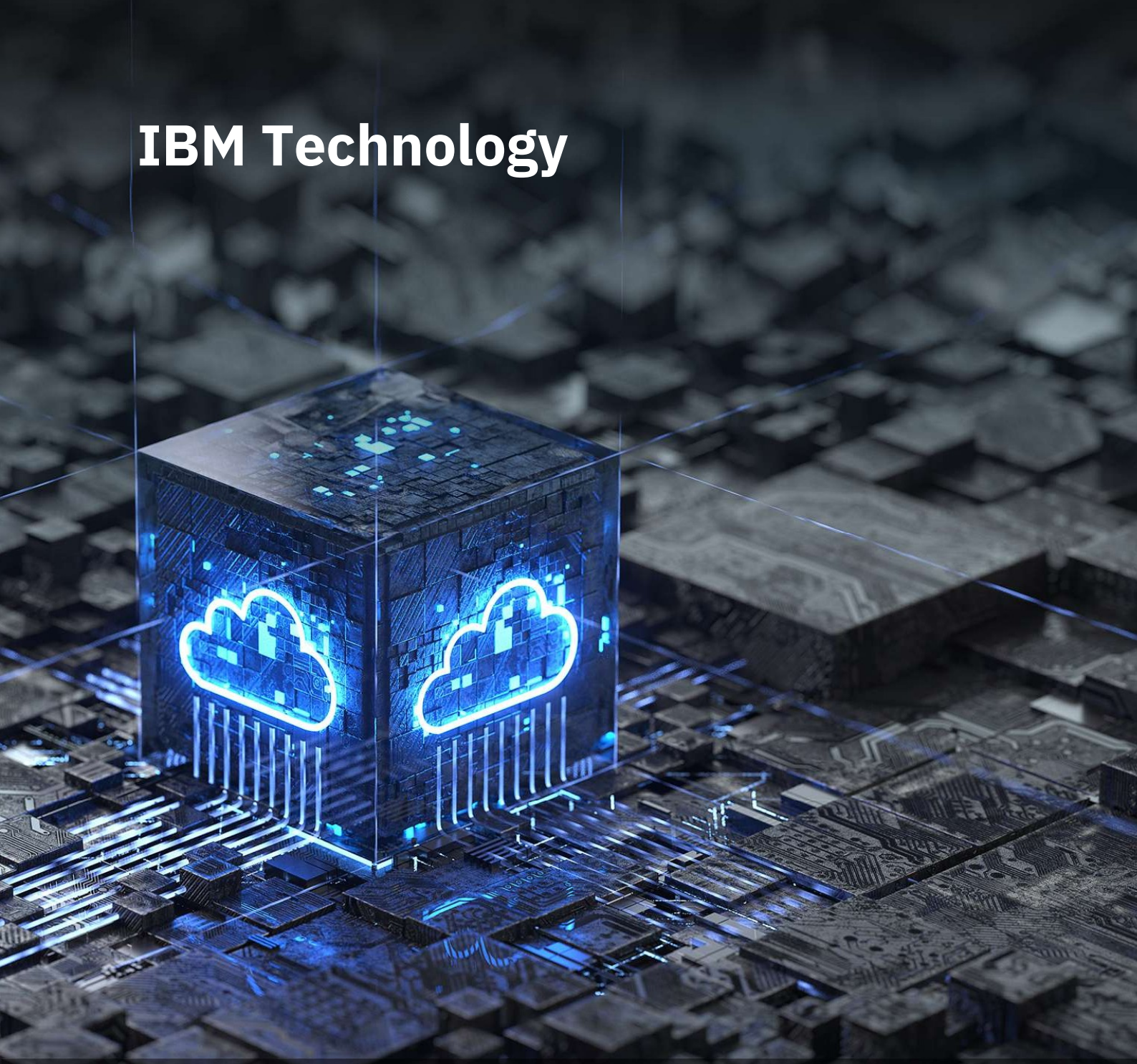
IBM Technology



G-Cloud 15
IBM – Verify Privilege

Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

IBM Security Verify Privilege

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

IBM Security Verify Privilege Cloud Service consists of the following 4 offerings, each includes one production environment:

IBM Security Verify Privilege Vault

Privilege Vault is a solution that allows Clients to:

- Establish a Secure Vault – Store privileged credentials in an encrypted centralized vault.
- Discover Privileges – Identify all services, applications, administrators, and root accounts.
- Manage Secrets – Provision & deprovision, ensure password complexity and rotate credentials.
- Delegate Access – Set up RBAC, workflow for access requests and approvals for third parties.
- Control Sessions – Implement session launching, proxies, monitoring and recording.

IBM Security Verify Privilege Manager

Privilege Manager is a solution that allows Clients to:

- Deploy a Single Agent – Discover application usage with admin rights, even on non-domain machines.
- Define Flexible Policies – Elevate, allow, deny, and restrict applications in just a few clicks with a policy wizard.
- Discover and Inventory – Find the most important applications that need to be addressed by Client's policies.
- Manage and Remove Local Admin Rights – Create rules to permanently define local group membership and automatically rotate credentials for non-human privileged accounts.
- Elevate Applications – Allow trusted applications to run, while maintaining a least privilege model.
- Improve IT Productivity – Automate bulk or repeatable operations. Reduce help desk tickets.
- Support Business Users – Allow people to access apps and systems they need automatically.

IBM Security Verify Privilege DevOps Vault

Privilege DevOps Vault helps Clients to protect privileges and reduce secret sprawl across cloud attack surface by:

- Establish a Secure DevOps Vault – Store privileged credentials in an encrypted, centralized SaaS-based vault in minutes.
- Centralize Secrets – Eliminate disparate vault instances with a platform-agnostic solution that enforces secure secrets access and provides complete auditing.
- Automate and Scale – Choose Client's automated interface (CLI and API) built for the speed and scale of DevOps pipelines and RPA deployments and tools.
- Manage Secrets for IaaS – Remove standing access to critical infrastructure with dynamic secrets for AWS, Azure and Google Cloud Platform.
- Issue Certificates – Issue X.509 and SSH certificates, which enables automated certificate signing and distribution.

IBM Security Verify Privilege Account Lifecycle Manager

IBM Security Verify Privilege Account Lifecycle Manager helps Clients automate the service account lifecycle. Some capabilities include:

- Discover Hidden Accounts – Find service accounts and understand their purpose.
- Establish Workflows – Delegate ownership with role-based permissions.

- Provision Accounts – Set up accounts seamlessly and automatically.
- Enforce Governance – Establish ownership and accountability for accounts.
- Decommission Accounts – Remove accounts without causing disruption.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Security Verify Privilege Vault for Business Users

IBM Security Verify Privilege Vault for Business Users offering is used to manage accounts not considered Privilege. These accounts can include individual or team application accounts and credentials. Examples of accounts not considered Privilege include email login, social media password, or productivity software credentials.

Privilege Vault provides the following entitlement per tenant:

- Storage of 4 TB
- Single Sign On and Multi Factor Authentication from the IBM Security Verify offering.
- A limit of 10,000 secrets, otherwise known as privileged credentials.
- 10 IBM Security Verify Privilege Vault Sites.
    - Each IBM Security Verify Privilege Vault Site includes 10 IBM Security Verify Privilege Vault Engines. Engine is a Windows Service which does discovery, password changing, and heartbeat. Each Engine belongs to a Site. Sites are logical groupings of work items. Every managed secret will have one Site. The Engine pulls work items from the Site for processing.

1.1.2 IBM Security Verify Privilege Vault for Privilege Users

IBM Security Verify Privilege Vault for Privilege Users offering is used to manage Privilege accounts; such as database server credentials, security appliance passwords, Cloud Service root keys, or any other IT infrastructure credentials.

Privilege Vault provides the following entitlement per tenant:

- Storage of 4 TB
- Single Sign On and Multi Factor Authentication from the IBM Security Verify offering.
- A limit of 10,000 secrets, otherwise known as privileged credentials.
- 10 IBM Security Verify Privilege Vault Sites.
    - Each IBM Security Verify Privilege Vault Site includes 10 IBM Security Verify Privilege Vault Engines. Engine is a Windows Service which does discovery, password changing, and heartbeat. Each Engine belongs to a Site. Sites are logical groupings of work items. Every managed secret will have one Site. The Engine pulls work items from the Site for processing.

1.1.3 IBM Security Verify Privilege Manager for Managed Client

The number of entitlements required for IBM Security Verify Privilege Manager for Managed Client is determined by the number of individual endpoint computers that the endpoint agent can be actively installed on.

1.1.4 IBM Security Verify Privilege Manager for Managed Server

The number of entitlements required for IBM Security Verify Privilege Manager for Managed Server is determined by the number of servers that the endpoint agent can be actively installed on.

1.1.5 IBM Security Verify Privilege DevOps Vault Production Subscription per Record

The number of entitlements required for IBM Security Verify Privilege DevOps Vault Production is determined by the number of passwords, encryption keys, digital certificates or other credentials stored in the production instance of IBM Security Verify Privilege DevOps Vault.

1.1.6 IBM Security Verify Privilege Account Lifecycle Manager for Users

The IBM Security Verify Privilege Account Lifecycle Manager offering is used to manage and automate the service account lifecycle.

Privilege Account Lifecycle Manager provides the following entitlement per tenant:

- One Account Lifecycle Manager Engine. This engine is a Windows Service that runs on the Client's hardware. It manages interactions between the Account Lifecycle Manager Cloud Service and the Client's Microsoft Active Directory.

1.1.7 IBM Security Verify Privilege Cloud Suite

IBM Security Verify Privilege Cloud Suite is a software-as-a-service (SaaS)-based solution that secures privileged access for servers in multi-cloud environments. It allows humans and machines to authenticate, enforcing least privilege with just-in-time privilege elevation, increasing accountability, and helps to reduce administrative access risk.

Security Verify Privilege Cloud Suite provides the following three core services:

- Cloud Authentication Service simplifies user authentication to servers from any directory service, including Active Directory, OpenLDAP, and other cloud directories, such as Azure AD. This enables secure access to Linux and Microsoft Windows virtual systems and containers and enforces adaptive multifactor authentication (MFA) for stronger identity assurance. This includes:
  - Multidirectory brokering
  - Machine identity, delegated machine credentials, and credential management
  - Authentication policy management
  - MFA at system login
- Cloud Privilege Elevation Service enforces the principle of least privilege across multi-cloud workloads to minimize the risk of a security breach. Administrators can request just-in-time privilege elevation for a limited time. This includes:
  - Consistent, dynamic, and automated security policy management
  - Just-in-time privilege
  - MFA at privilege elevation
- Cloud Audit and Monitoring Service helps with compliance and incident response by providing auditing features and tying activities to an individual identity. It identifies abuse of privilege, helps to counter attacks, and assists with regulatory compliance by providing a detailed audit trail and video recordings that capture all privileged activity. This includes:
  - Advanced, host-based session recording, auditing, and reporting
  - Gateway session recording, monitoring, and control

1.2 Optional Services

The Client may select from the following available add-ons.

1.2.1 IBM Security Verify Privilege Vault Sites

IBM Security Verify Privilege Vault Sites add-on is used to expand the number of Sites included in the Cloud Service.

1.2.2 IBM Security Verify Privilege Vault Engines

IBM Security Verify Privilege Vault Engines add-on is used to expand the number of Engines included in the Cloud Service.

1.2.3 IBM Security Verify Privilege Vault Analytics

IBM Security Verify Privilege Vault Analytics provides risk-based user behavior alerts for activity within IBM Security Verify Privilege Vault. This Service can be configured to perform various response actions when an alert occurs.

1.2.4 IBM Security Verify Privilege Vault for Business Users Non-Production

IBM Security Verify Privilege Vault for Business Users Non-Production offering is a separate instance of the IBM Security Verify Privilege Vault for Business Users offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.5 IBM Security Verify Privilege Vault for Privileged Users Non-Production

IBM Security Verify Privilege Vault for Privileged Users Non-Production offering is a separate instance of the IBM Security Verify Privilege Vault for Privileged Users offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.6 IBM Security Verify Privilege Manager Non-Production for Managed Client

IBM Security Verify Privilege Manager Non-Production for Managed Client offering is a separate instance of the IBM Security Verify Privilege Manager for Managed Client offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.7 IBM Security Verify Privilege Manager Non-Production for Managed Server

IBM Security Verify Privilege Manager Non-Production for Managed Server offering is a separate instance of the IBM Security Verify Privilege Manager for Managed Server offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.8 IBM Security Verify Privilege DevOps Vault Non-Production Subscription per Record

The number of entitlements required for IBM Security Verify Privilege DevOps Vault Non-Production is determined by the number of passwords, encryption keys, digital certificates or other credentials stored in the non- production instance of IBM Security Verify Privilege DevOps Vault.

1.2.9 IBM Security Verify Privilege Account Lifecycle Manager Engines

The Account Lifecycle Manager Engine is a Windows Service that runs on a machine in the Client's environment. The Engine service manages interactions between the Account Lifecycle Manager Cloud Service and the Client's Microsoft Active Directory. This add-on is used to enable High Availability or an additional Microsoft Active Directory domain.

1.2.10 IBM Security Verify Privilege Account Lifecycle Manager Non-Production for Users

The IBM Security Verify Privilege Account Lifecycle Manager Non-Production for Users offering is a separate instance of IBM Security Verify Privilege Account Lifecycle Manager for Users offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

1.2.11 IBM Security Verify Privilege Vault Additional Secrets (Pack of 1000 Secrets)

IBM Security Verify Privilege Vault Additional Secrets (Pack of 1000 Secrets) enables a Client using IBM Security Verify Privilege Vault offerings to add secrets when the limit of 10,000 is insufficient for the Client's organization.

1.2.12 IBM Security Verify Privilege Cloud Suite Non-Production

IBM Security Verify Privilege Cloud Suite Non-Production offering is a separate instance of the IBM Security Verify Privilege Cloud Suite offering that a Client may only use for internal non-production activities, including but not limited to testing, performance tuning, fault diagnosis, internal benchmarking, staging quality assurance activity and/or developing internally used additions or extensions to the Cloud Service using published application programming interfaces.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM’s processing of personal data on behalf of Client.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=4B8D1F20C00511E9908EB999AAEAE31E

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

Non-production Cloud Service instances are not eligible for Service Level Agreements (SLA).

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

3.2.1 Technical Support for All Non-Production Instances

Support for non-production instances is available from 8 AM to 8 PM in any of the following four home regions: Washington, DC, London, United Arab Emirates, and the Philippines. In addition, severity levels and response times as laid out in the IBM Cloud Service overview will not be applied to Non-Production Instance support cases.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Authorized User is a unique user authorized to access to the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device, or application server) through any means.
- Instance is each access to a specific configuration of the Cloud Services.
- Managed Client Device is any device that requests or receives execution commands, procedures or applications from a server environment managed by the Cloud Services.
- Managed Server is a physical computer or device (such as a blade or rack-mounted device) that is comprised of processing units, memory and input/output capabilities, and that executes requested procedures, commands or applications for users or Client devices managed by the Cloud Services.
- Record is a set of unique attributes for a specific item that is managed by, processed by, or related to the use of the Cloud Service. Unique attributes can include secrets, passwords, encryption keys, digital certificates, or any other credential stored in the Cloud Service.
- Virtual Server is comprised of processing units, memory and input/output capabilities that executes requested procedures, commands or applications made available to the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.