IBM Security Privileged Identity Manager
Version 2.1.0

# *Planning and Deploying Guide*

IBM Security Privileged Identity Manager
Version 2.1.0

# *Planning and Deploying Guide*

IBM

**Note**

Before using this information and the product it supports, read the information in Notices.

**Edition notice**

**Note: This edition applies to Version 2.1.0 of** *IBM Security Privileged Identity Manager* **(product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.**

# Contents

# Figures

# Tables

# Chapter 1. Planning usage scenarios

The following scenarios describe some of the common scenarios that users and administrators do in IBM® Security Privileged Identity Manager to complete daily tasks.

Throughout this section, the following personas are used in scenarios to describe scenarios according to their role by using IBM Security Privileged Identity Manager:

- Vic Green (Privileged Administrator)
- James Smith (Privileged User)

For more details on each role, see Roles and scenarios.

## Scenarios: Administration and on-boarding credentials (Privileged Administrator)

The following scenarios are described from the role of a Privileged Administrator for the on-boarding of credentials.

In this scenario, Vic Green (Privileged Administrator) owns a set of credentials. The following scenarios are methods that he can use to onboard credentials with IBM Security Privileged Identity Manager.

| Persona | Scenario |
|---|---|
| Vic Green (Privileged Administrator) | **On-boarding credentials with Service Center**<br>Vic can onboard and manage credentials in the Privileged Identity Manager Service Center. He can onboard credentials as "exclusive" (credential that requires check-out) or as "non-exclusive" (credentials that do not require check-out) and can assign entitlements on each credential.<br>See "Adding Credentials with Service Center" in the *IBM Security Privileged Identity Manager Administrator Guide*. |
| | **On-boarding credentials with bulk upload**<br>With bulk upload, Vic can onboard credentials by importing entries from a CSV file. IBM Security Privileged Identity Manager uses the settings that are indicated a CSV file to add or update credentials.<br>Vic uploads the CSV file with the Administrative console to onboard credentials in bulk.<br>This method of on-boarding credentials is suggested for initial deployments when there are a lot of credentials to onboard.<br>See "Uploading a CSV file with the administrative console" and "Bulk loading" in the *IBM Security Privileged Identity Manager Administrator Guide*. |
| | **On-boarding credentials with REST APIs**<br>REST APIs are useful for developing your own integration scenarios, such as on-boarding users. Vic can use the REST APIs to automatically onboard credentials when new systems are provisioned and removed from IBM Security Privileged Identity Manager.<br>This method of on-boarding is also suggested for initial deployments when there are a lot of credentials to onboard.<br>See REST APIs for IBM Security Privileged Identity Manager. |

## Scenarios: Shared access to privileged identities (Privileged Users and Privileged Administrators)

The following scenarios are described from the role of a Privileged Administrator and from the role of a Privileged User. Each privileged credential check-in and check-out scenario is designed to fit different deployment environments and requirements.

Both the Privileged Administrator and Privileged User can check-in and check-out credentials to access resources by using one of the following methods:

**Automatic check-in and check-out with Privileged Access Agent**

Performs automatic check-in and check-out with single sign-on to target systems.

**Manual check-in and check-out with self-service console**

- Manually check-out credentials to view the password.
- Manually check-out credentials and initiate Privileged Session Gateway sessions.

The following personas are used in the scenarios:

- Vic Green (Privileged Administrator)
- James Smith (Privileged User)

| Description | Scenario |
|---|---|
| This scenario is applicable for the following:<br>• Credentials or resources, where users cannot or do not use Privileged Access Agent.<br>• Password is required for manual log on to physical consoles.<br>• Logging on to target systems that are not supported by Privileged Session Gateway. | **Scenario 1: Manual check-in and check-out (View Password) for connected exclusive credentials**<br>• James manually checks out an exclusive credential from the self-service console to view the password. He uses this password to manually log on to target systems. After he is done, he checks in the credential.<br>• Since the password is visible to James, it is recommended that Vic configures IBM Security Privileged Identity Manager to rotate the password upon each credential check-in. |
| This scenario is applicable for when exclusive access to a credential needs to be assured for auditing and tracking purposes. | **Scenario 2: Automated check-in and check-out with Privileged Access Agent for exclusive credentials**<br>• James uses Privileged Access Agent to perform automatic check-in and check-out credentials to single sign-on into the target systems.<br>• For connected credentials, Vic configures IBM Security Privileged Identity Manager to rotate the password upon each check-in or periodically. With exclusive credentials, system administrators can keep track of any suspicious activities that are performed by a shared credential at a certain time for a specific user.<br>• For credentials that are not connected, Vic manually rotates the credential passwords at the target resource and updates new passwords into IBM Security Privileged Identity Manager accordingly. In this instance, it is recommended that he configures the credential settings to disable the **Display password to user** option in the Privileged Identity Manager Service Center. |
| This scenario is applicable for when there is only one single privileged credential for the resource and concurrent access needs to be supported. Privileged Access Agent automates log on without revealing the credential password to the user. | **Scenario 3: Automated check-in and check-out with Privileged Access Agent for non-exclusive credentials**<br>• James uses Privileged Access Agent to perform automatic check-in and check-out credentials to single sign-on into the target systems.<br>• For connected credentials, Vic configures IBM Security Privileged Identity Manager to rotate the password upon each check-in or periodically.<br>• For credentials that are not connected, Vic manually rotates the credential passwords at the target resource and updates new passwords into IBM Security Privileged Identity Manager accordingly. In this instance, it is recommended that he configures the credential settings to disable the **Display password to user** option in the Privileged Identity Manager Service Center. |

| Description | Scenario |
|---|---|
| This scenario is applicable for credentials of resource types that the Privileged Session Gateway can connect to, where exclusive access needs to be assured for auditing and tracking purposes. | **Scenario 4: Automated log on with Privileged Session Gateway for exclusive credentials**<br>• James logs on to the self-service console to use a credential to automatically connect to the target systems with Privileged Session Gateway.<br>• For connected credentials, Vic configures IBM Security Privileged Identity Manager to rotate the password upon each check-in or periodically. With exclusive credentials, system administrators can keep track of any suspicious activities that are performed by a shared credential at a certain time for a specific user.<br>• For credentials that are not connected, Vic manually rotates the credential passwords at the target resource and updates new passwords into IBM Security Privileged Identity Manager accordingly. In this instance, it is recommended that he configures the credential settings to disable the **Display password to user** option in the Privileged Identity Manager Service Center. |
| This scenario is applicable for when there is only one single privileged credential for the resource and concurrent access needs to be supported. Privileged Session Gateway automates log on without revealing the credential password to the user. | **Scenario 4: Automated log on with Privileged Session Gateway for non-exclusive credentials**<br>• James logs on to the self-service console to use a credential to automatically connect to the target systems with Privileged Session Gateway.<br>• For connected credentials, Vic configures IBM Security Privileged Identity Manager to rotate the password upon each check-in or periodically.<br>• For credentials that are not connected, Vic manually rotates the credential passwords at the target resource and updates new passwords into IBM Security Privileged Identity Manager accordingly. In this instance, it is recommended that he configures the credential settings to disable the **Display password to user** option in the Privileged Identity Manager Service Center. |

## Scenarios: Privileged Session Gateway usage (Privileged Users)

Learn how a Privileged User can use the Privileged Session Gateway to perform system administration tasks efficiently on many SSH-enabled hosts.

### Scenario: Concurrent access to multiple SSH-enabled resources for an external contractor

Rajeev is an external contractor and a Privileged User at JK Enterprises. His task is to perform routine system administration over SSH on multiple remote hosts. In order to perform this task, he wants access to multiple concurrent sessions in the same web browser.

*Table 1. Usage scenario for Privileged Session Gateway*

| Task | Reference |
|---|---|
| As a Privileged User, Rajeev gets credentials to log on to an SSH-enabled resource through the self-service console. | • Initiating a session with credentials that require check-out<br>• Initiating a session with credentials that do not require check-out |

Table 1. Usage scenario for Privileged Session Gateway (continued)

| Task | Reference |
|---|---|
| He launches multiple sessions using the same credential. | |
| Rajeev requires the ability to copy and paste text between some of the sessions. | Clipboard function |
| As Rajeev continues to initiate different connections to more SSH-enabled resources, he decides to check his list of available sessions. | • Listing sessions with the self-service console |
| After Rajeev completes his administration tasks, he ends his session to the SSH-enabled resources. | Ending your own session |

# Chapter 2. Planning for deployment

There are several factors that affect the successful deployment of IBM Security Privileged Identity Manager. You must plan carefully. Know what you have, need and must do to successfully install or upgrade, or ensure the high availability and disaster recovery of IBM Security Privileged Identity Manager.

You can use the following guidelines on how to start planning for IBM Security Privileged Identity Manager deployment:

## Deployment scope and size

You can deploy IBM Security Privileged Identity Manager in different topology configurations. The deployment size determines the complexity and duration of the deployment.

Small deployments require less resources and are easier to deploy. Medium to large-scale deployments require more time and resources, compared to small scale deployments. These deployments provide greater flexibility, can handle higher loads, and support a larger number of users.

The combination of the following factors determine the size of a deployment:

- Number of privileged users
- Number of privileged IDs for check-out and check-in for Shared access
- Number of concurrent users expected
- Types of target resources and identity providers
- Number of applications (and types) and associated application identity for Application identity management

### Simple deployments

In this example of a simple deployment, out-of-the-box adapters are used to handle external connections to managed resources.

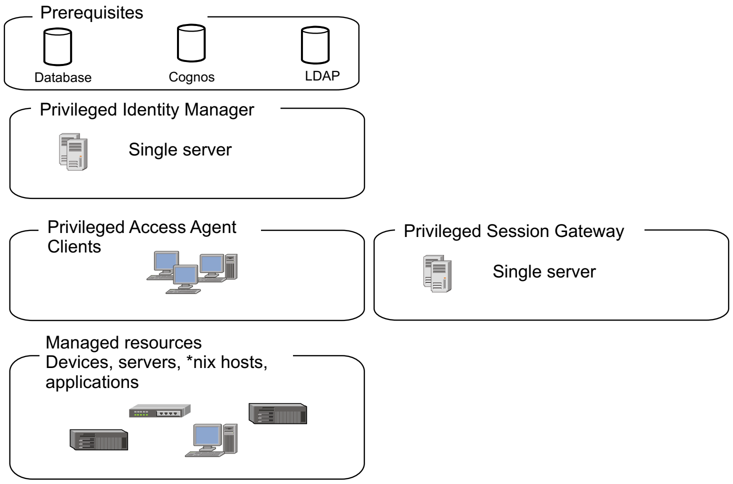

*Figure 1. Simple deployment suitable for a proof-of-concept.*

## Standard deployments

In a standard deployment, the variety of supported identity providers are extended by installing non out-of-the-box adapters on an external IBM Security Directory Integrator host. You add non-out-of-the-box adapters to support a larger variety of managed resources. The solution is clustered for high availability.

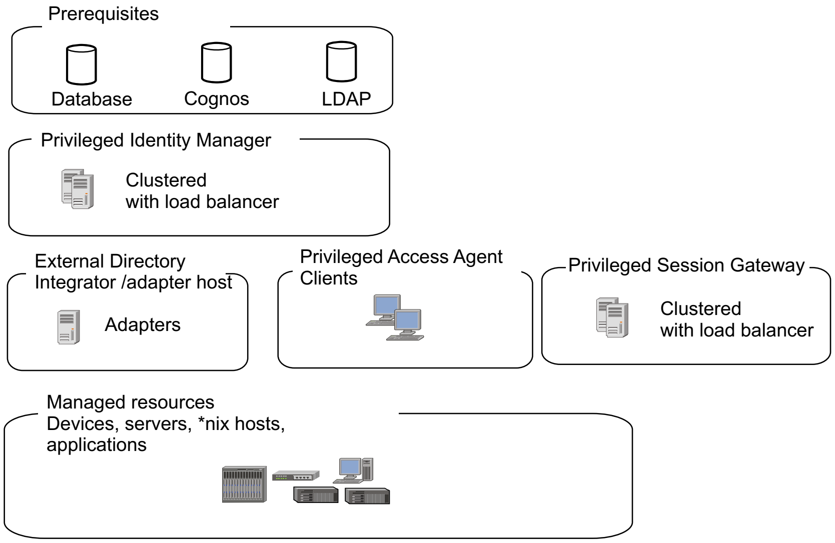

*Figure 2. Standard deployment*

## Advanced deployments

In an advanced deployment, IBM Security Privileged Identity Manager uses multiple servers in clusters or failover configurations to host the data tier. The database is clustered, and the LDAP servers are replicated.

In work environments that provide virtualized desktop or application infrastructure, you can also deploy Privileged Access Agent on a gateway. For more information, see *IBM Security Privileged Identity Manager Access Agent on a Gateway Guide*.

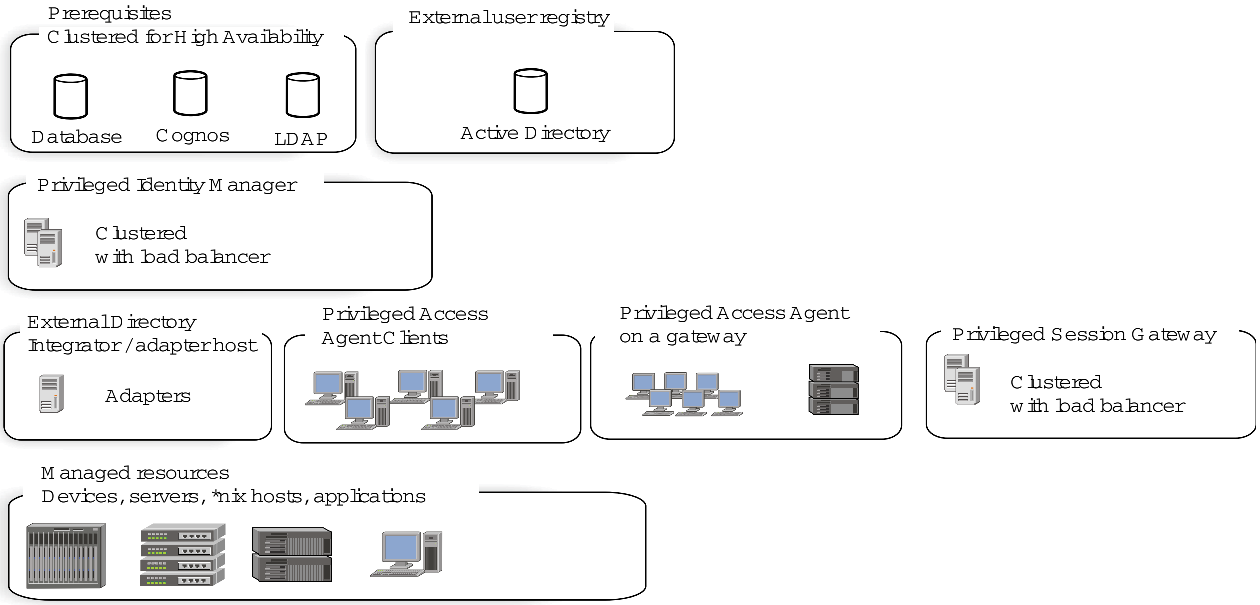

*Figure 3. Advanced deployment with multiple servers and failover configurations.*

The example shows integration with different solutions to extend the capabilities of IBM Security Privileged Identity Manager. Users are provisioned and on boarded from IBM Security Identity Manager. Multifactor authentication for privileged identities is provided by setting up an IBM Security Access Manager reverse proxy.

For more information, see “Integration with IBM Security Access Manager” in the *IBM Security Privileged Identity Manager Product Overview Guide*.

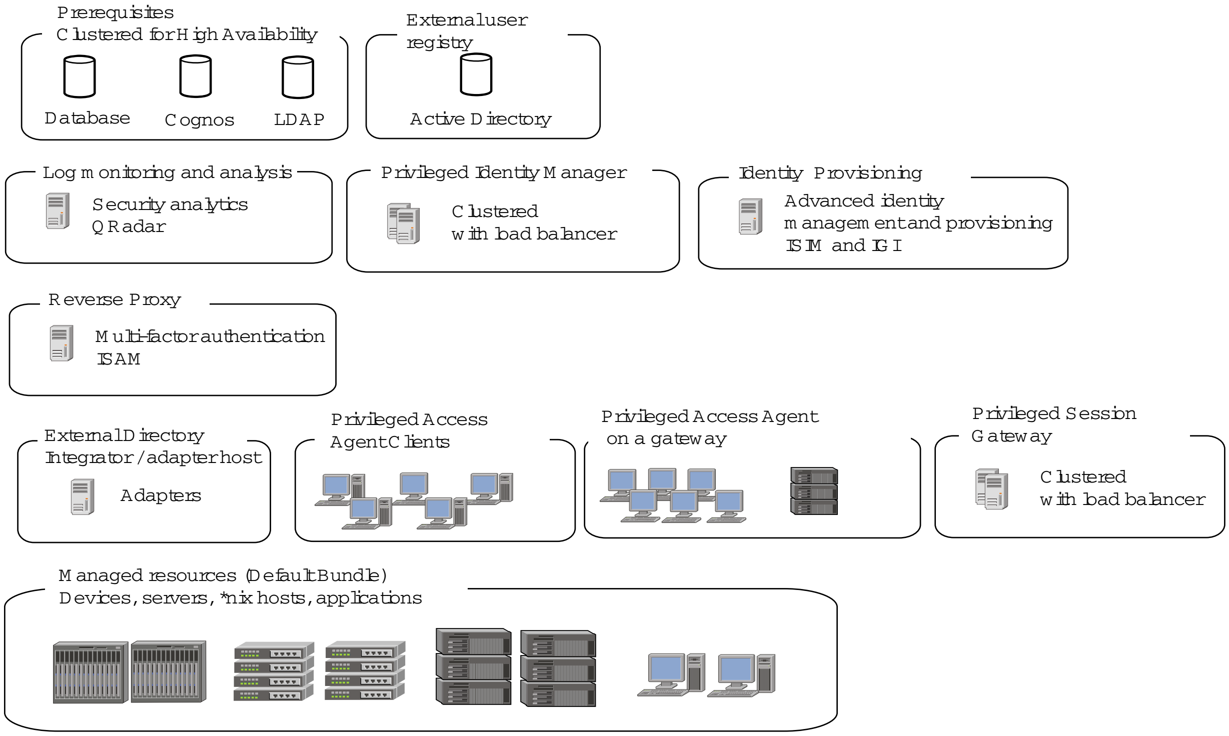
Prerequisites
Clustered for High Availability
Database
Cognos
LDAP
External user registry
Active Directory
Log monitoring and analysis
Security analytics
QRadar
Privileged Identity Manager
Clustered with load balancer
Identity Provisioning
Advanced identity management and provisioning
ISIM and IGI
Reverse Proxy
Multi-factor authentication
ISAM
External Directory Integrator/adapter host
Adapters
Privileged Access Agent Clients
Privileged Access Agent on a gateway
Privileged Session Gateway
Clustered with load balancer
Managed resources (DefaultBundle)
Devices, servers, *nix hosts, applications

*Figure 4. Advanced deployment that integrates with more solutions such as IBM Security Access Manager to provide multi-factor authentication.*

An external IBM Security Directory Integrator adapter host, allows you to extend IBM Security Privileged Identity Manager support on other managed resources or devices with identity providers that are not preconfigured with the virtual appliance.

The Privileged Access Agent client is also deployed on a terminal server. Deploying clients on the terminal server provides privileged access to certain users that are accessing endpoints through a remote gateway without having to install an agent on their desktops.

## Deployment phases

Deploy IBM Security Privileged Identity Manager in phases especially for moderate and complex deployments.

### Test phase

In the test phase, the test team tests the software based on the documented procedures and reports any issues found to the development team.

### Pilot phase

The pilot phase involves deploying IBM Security Privileged Identity Manager to a relatively small number of users. The purpose of this phase is to discover and address any issues in the installation, configuration, and administration procedures.

In this phase, consider the following factors:

- Number of privileged users: Consider the location, language, and job role of the privileged user.
- Types of target resources and identity providers
- Number of applications (and types) and application identities associated for Application identity management

### Production phase

The production phase takes place after the pilot phase proves that the IBM Security Privileged Identity Manager deployment to the selected users is stable.

In the production phase, IBM Security Privileged Identity Manager is deployed to the entire scope of users. The same procedures that are used in the pilot phase, are used in the production phase.

## Deployment considerations

Several factors affect the successful deployment of IBM Security Privileged Identity Manager.

Learn more about what requirements you must plan and account for before you deploy IBM Security Privileged Identity Manager in a production environment.

### Planning checklist

The following table describes the general steps for planning your deployment.

*Table 2. Planning checklist*

| Done | Step |
|---|---|
| | Review the components for IBM Security Privileged Identity Manager to determine the components that you might want to install. |
| | Review the deployment topologies that IBM Security Privileged Identity Manager supports to determine which topology is most suited within your network. |
| | Review licensing requirements for your environment. |
| | Review hardware and software requirements for IBM Security Privileged Identity Manager, and then install, and configure all required hardware and software. Some components are optional. |
| | Review the security requirements for IBM Security Privileged Identity Manager. Plan your firewall and load balancer configuration. |
| | Review the installation guide for the right installation type and steps to best fit your deployment requirements. |

### Considerations for each aspect of a deployment

*Table 3. Deployment considerations*

| Category | Considerations |
|---|---|
| **Organization structure** | What is the high-level domain structure? |
| **Users** | Can you use an external Active Directory for IBM Security Privileged Identity Manager user authentication? |

*Table 3. Deployment considerations (continued)*

| Category | Considerations |
|---|---|
| **Deployment architecture** | • Will the Privileged Access Agent be deployed?<br>• Will the Privileged Access Agent be deployed to the Citrix Gateway or to virtual desktop infrastructure?<br>• Will the Privileged Session Gateway be deployed?<br>• How many concurrent user sessions with session recording are expected?<br>If more concurrent users are expected, consider scaling the cluster horizontally by adding more nodes.<br>• What are the high availability and disaster recovery requirements?<br>If you set up a load balanced cluster, is there a Layer 7 Load Balancer available to front it?<br>If you set up a data tier, is there redundancy built in? |
| **Default policies** | • What is the default shared access policy? For example, exclusive credentials and non-exclusive credentials.<br>• What is the default password policy?<br>• What is the default access entitlement policy? |
| **Resources and credentials for shared access check in and check out** | • Identify a group of hosts and applications that are targeted for IBM Security Privileged Identity Manager management.<br>You can use a network mapping or discovery tool to discover what hosts or apps are available in your network.<br>• Identify owners or Privileged Administrators that will oversee each group of resources or identities to be placed into IBM Security Privileged Identity Manager domains.<br>• Work with Privileged Administrators to enumerate the identities to be on-boarded into IBM Security Privileged Identity Manager. Gather the required information such as check-in, check-out, and adapter settings. Gather information about credentials and resources into suitable CSV files for bulk upload. |
| **Resources and credentials for App ID** | • Identify groups of hosts and applications that are targeted for IBM Security Privileged Identity Manager.<br>For example, you can run `discovery` to discover what hosts or apps are available.<br>• Identify owners or Privileged Administrators that will oversee each group of resources or identities to be placed into PIM domains. |
| **On-boarding strategy** | • For users, use a feed file. For example: Active Directory, LDAP, or a CSV feed.<br>• For each major data type (Identity Providers, Resource, Credential, Credential Pools, Access), choose between manual creation, CSV bulk-load, or REST API bulk-load. |

## Upgrades

You can upgrade IBM Security Privileged Identity Manager with one of the following ways:

**Fix packs**

Fix packs typically contain minor changes, fixes, and enhancements.

Fix packs are applied to the virtual appliance from the virtual appliance management console or through an SSH command line interface. In a cluster, the fix pack must be applied to each virtual appliance node.

**Firmware upgrades**

Firmware upgrades typically contain significant changes, such as major feature enhancements. These upgrades are typically published as firmware upgrades in the form of PKG files. You can download the files from Fix Central.

You can copy the PKG package to a USB drive or use the File Upload tool. The USB drive is attached as a virtual USB drive to the remote virtual appliance through the hypervisor console, such as VMware vSphere. You apply the package to the virtual appliance with Secure Shell. Alternatively, you can also use the File Upload tool. The tool uploads packages over HTTPS into the virtual appliance.

A firmware upgrade preserves existing configurations within the virtual appliance and existing data in the external data tier. Any data tier schema changes that are introduced in newer versions are automatically applied on the external data tier during the virtual appliance upgrade process.

To upgrade the Privileged Session Gateway, you can install new instances that co-exist with older instances on the same computer. You can then transfer traffic to the new instances after traffic to older instances stop. See Upgrade the Privileged Session Gateway.

Always back up the virtual appliance and the data tier. See the specific upgrade package release notes for exceptions or limitations. Instructions for upgrades can vary from one release to the next.

## Monitoring

Each IBM Security Privileged Identity Manager instance exposes a monitoring HTTPS URL that an external monitoring system can periodically poll to check on the status of various application components. For more information, see Monitoring URLs.

For SNMP monitoring, each IBM Security Privileged Identity Manager virtual appliance can be configured to allow SNMP queries on various OS-level SNMP properties, such as CPU and RAM utilization.

Monitor data tier components by using the typical monitoring features that are provided by the component such as IBM Security Directory Server and DB2®.

## Disaster recovery

IBM Security Privileged Identity Manager supports an active-passive configuration for disaster recovery. Set up a standby IBM Security Privileged Identity Manager deployment in a disaster recovery site that is separate from the production site.

First, set up a warm standby of the IBM Security Privileged Identity Manager data tier at the disaster recovery site. For DB2, use DB2 HADR technology to replicate the changes from the production IBM Security Privileged Identity Manager database to the standby database. For IBM Security Directory Server, set up LDAP replication between the production server and its replace LDAP server at the disaster recovery site.

## Security

You can import trusted CA certificates for securing network connections such as:

- The external IBM Security Directory Server instance that is hosting the IBM Security Privileged Identity Manager LDAP store over HTTPS or LDAPs.
- The external Active Directory controller for authentication or HR feeds.
- The external Identity Adapters (for example, Win AD and Win Local agents or IBM Security Directory Integrator RMI Dispatcher).

After you import the trusted certificates, go to the appropriate IBM Security Privileged Identity Manager administration configuration tool to configure the SSL or TLS connections for the respective outgoing connections.

IBM Security Privileged Identity Manager virtual appliance is bundled with a self-signed CA that is used to sign the TLS/SSL certificate for each IBM Security Privileged Identity Manager virtual appliance node upon instantiation. The TLS/SSL certificate self-renews before it expires. You can also import the certificates to replace the bundled SSL certificates. The virtual appliance administrator must prepare the externally signed certificate (with private keys) in a password-protected PKCS#12 file. Then, the virtual appliance administrator uploads the file to the virtual appliance, and marks the certificate as the default certificate for HTTPS communications.

In a typical highly available IBM Security Privileged Identity Manager deployment, the virtual appliance nodes must be fronted by a Layer 7 Load Balancer (Reverse Proxy). All requests from Privileged Users and IBM Security Privileged Identity Manager clients must be directed to this Load Balancer. It is important to ensure that the Load Balancer use certificates and cipher suites that meet your organization's security requirements.

# Chapter 3. Planning for high availability

IBM Security Privileged Identity Manager virtual appliance with a load balanced cluster provides not only the expected high availability but also provides scalability.

## Load Balancer settings and requirements

Load Balancing is a technique that helps in the distribution of requests or tasks between two or more virtual appliances in a predefined cluster. Each virtual appliance in this cluster is called a node. Use of multiple nodes in such a cluster increases reliability and availability through redundancy.

## Load Balancer requirements

The most common mechanism to make a highly available deployment is to add a Load Balancer that distributes user requests to underlying servers. This deployment locks down any direct access to individual servers. In addition to making a highly available deployment of the IBM Security Privileged Identity Manager virtual appliance, it also provides horizontal scalability.

You can scale the cluster horizontally according to the number of concurrent users that you expect.

See Figure 5.

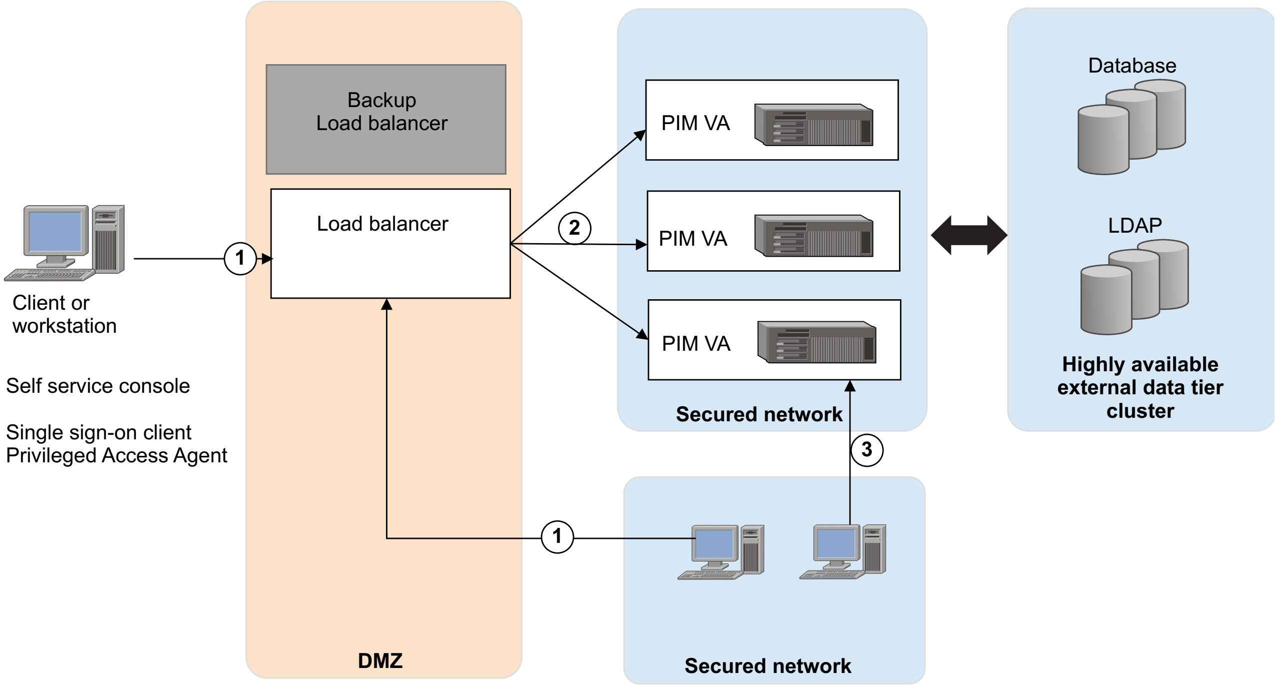

*Figure 5. Deployment diagram of a typical Load Balancer in a customer environment*

As shown in Figure 5 on page 15, provide one or more backup Load Balancers or routers to avoid the Load Balancer itself from becoming a single point of failure.

The Load Balancer can be a dedicated hardware or software node that can route incoming requests to an IBM Security Privileged Identity Manager virtual appliance. This condition is true irrespective of whether the requests are coming from inside or outside a company network. See the request that is numbered as 1 in the diagram. Since these requests typically contain sensitive information such as user IDs or passwords, both the traffic paths must be over SSL. For example, see requests 1 and 2. The client request over SSL (marked #1) ends at the Load Balancer and a new SSL request (marked #2) is sent to a virtual appliance. Designated virtual appliance management consoles in the secured network can establish a direct connection requests to the virtual appliance (marked #3)

### Load Balancer installation requirements

The Load Balancer must meet the following requirements:

- Choose `Layer-7` Load Balancer for this installation. `Layer-4` Load Balancers do not provide the required function and must not be used for this architecture.
- The Load Balancer must contain a valid SSL certificate for the Privileged Access Agent to connect. For a self-signed certificate, the Root CA certificate with which the Load Balancer certificate is signed must be imported in the client truststore.
- The Load Balancer must be able to send separate SSL requests for each of the incoming requests.

### Load Balancer configuration requirements

In the Load Balancer configuration:

- Enable Session Affinity for the Load Balancer. Use a Load Balancer with session affinity to route the traffic for the same client session to the same virtual appliance.
- Set the client host IP into the `X-Forwarded-For HTTP header`. The IBM Security Privileged Identity Manager virtual appliance must know the client IP for its audit logs.
- The Load Balancer must detect unresponsive virtual appliances and stop directing any traffic to them.
- As shown in Figure 5 on page 15, keep one or more of the Load Balancer backups ready to avoid the Load Balancer being a single point of failure.
- Set the Load Balancer to allow underscores in request headers. For example, set the value of the `underscores_in_headers` custom header directive to `on` in Nginx.

## Planning for high availability with IBM Security Access Manager

Plan for a high availability deployment with IBM Security Access Manager reverse proxy instances.

When there are multiple back-end servers, session affinity in IBM Security Access Manager can only be configured for the same junction.

To achieve high availability when IBM Security Access Manager is fronting IBM Security Privileged Identity Manager, you must ensure that all subsequent requests across the different junctions from a IBM Security Privileged Identity Manager client during the same session are forwarded to the same IBM Security Privileged Identity Manager virtual appliance.

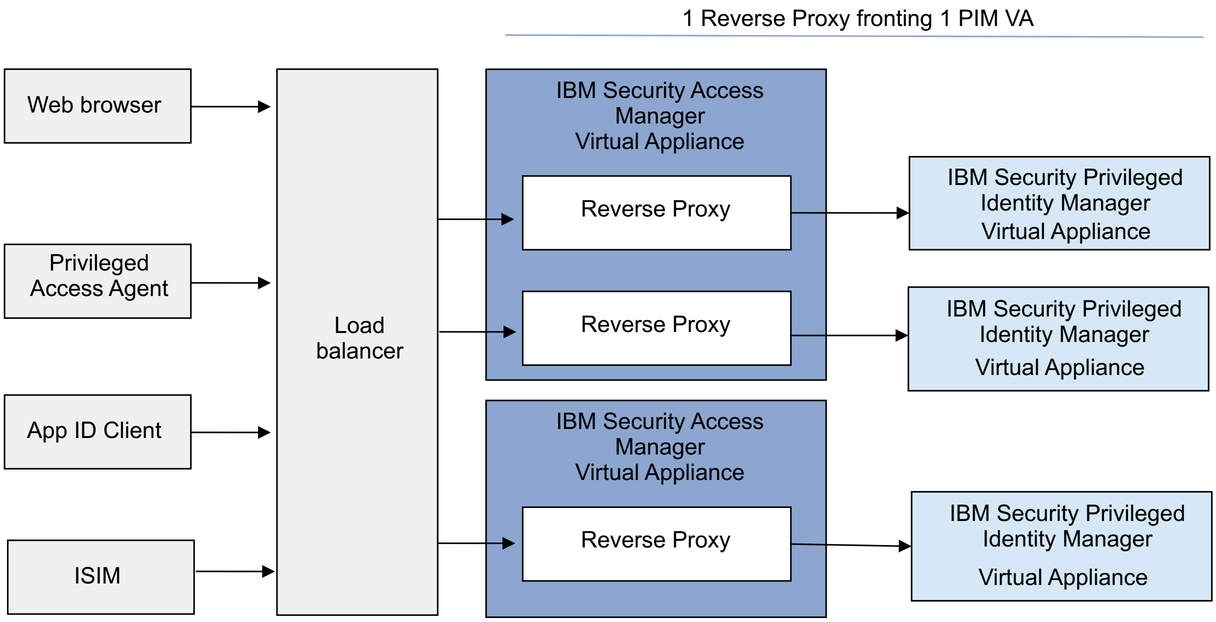
1 Reverse Proxy fronting 1 PIM VA
Web browser
Privileged Access Agent
App ID Client
ISIM
Load balancer
IBM Security Access Manager Virtual Appliance
Reverse Proxy
Reverse Proxy
IBM Security Access Manager Virtual Appliance
Reverse Proxy
IBM Security Privileged Identity Manager Virtual Appliance
IBM Security Privileged Identity Manager Virtual Appliance
IBM Security Privileged Identity Manager Virtual Appliance

*Figure 6. High availability with IBM Security Access Manager reverse proxy*

The suggested configuration consists of the following elements:

- 1 IBM Security Access Manager Reverse Proxy fronting 1 IBM Security Privileged Identity Manager virtual appliance.
- 1 IBM Security Access Manager virtual appliance can have more than 1 IBM Security Access Manager Reverse Proxy depending on the virtual appliance capacity.
- A Load Balancer with session affinity enabled to manage the IBM Security Access Manager Reverse Proxies.
- In the PIM VA Load Balancer Configuration, set the Load Balancer DNS to point to the Load Balancer.

**Note:** When there is only one Reverse Proxy fronting the IBM Security Privileged Identity Manager virtual appliance and there is no separate Load Balancer, configure the IBM Security Privileged Identity Manager virtual appliance Load Balancer to point to the Reverse Proxy.

## Planning for high availability with the Privileged Session Gateway

For high availability, you can deploy multiple instances of the Privileged Session Gateway in the same or different Linux machines

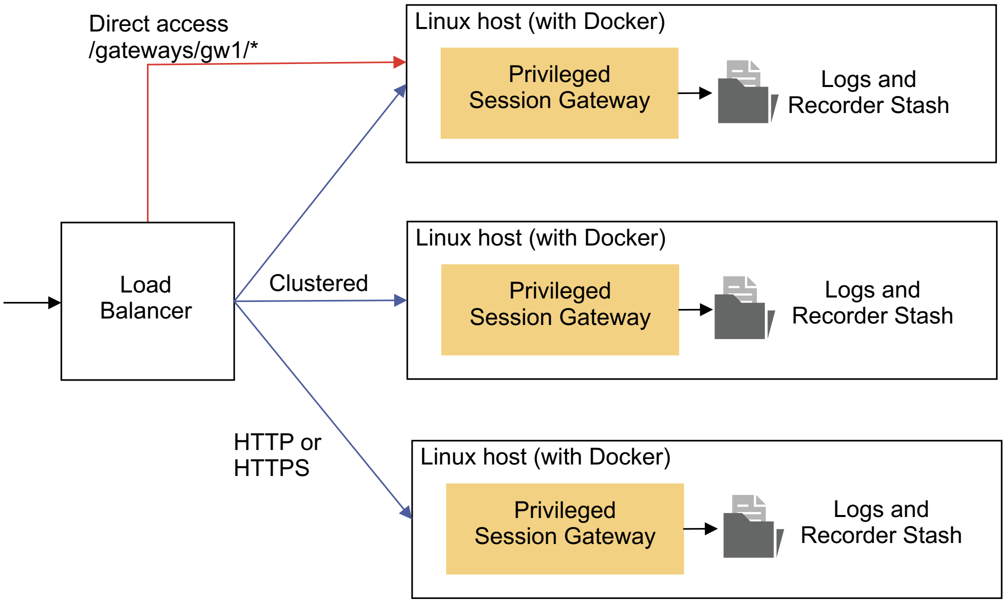

*Figure 7. Load balancer distributes traffic to individual instances in a cluster*

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

**Applicability**
These terms and conditions are in addition to any terms of use for the IBM website.

**Personal use**
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

**Commercial use**
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

**Rights**
Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

## Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

## Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.

Printed in USA