Introduction

Ironsphere protects privileged accounts, controls privileged user access, enforces segregation of duties, and logs user sessions to ensure that privileges are used only for legitimate business purposes. Ironsphere has a proven track record of success in bringing up operational efficiency with its fast deployment and enhanced capabilities.

Ironsphere further enhances the operational efficiency with multitenancy capabilities, providing multiple isolated and virtually separated Ironsphere services running on a single instance, to serve multiple departments in an organization, or in different organizations, as if they have their own dedicated instance.
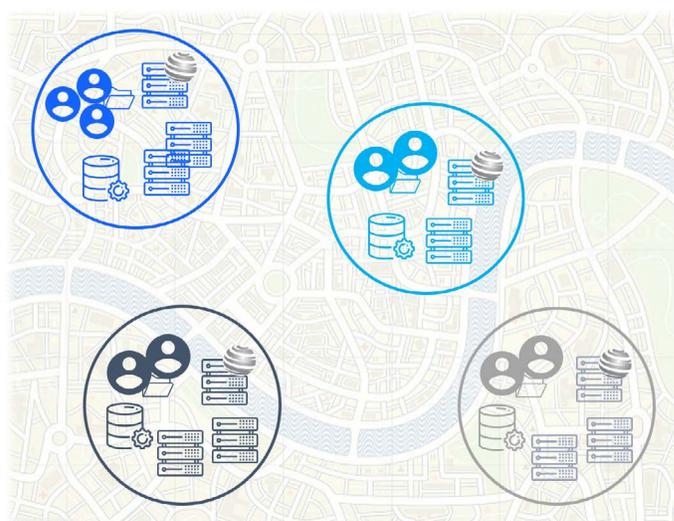
Challenge

An organization's IT department or a managed service provider aiming to implement a privileged management access solution must implement it per business unit, or per customer, which requires setting up different instances of the same application, consuming additional resources for every deployment.

Ironsphere's Multitenancy added-value capabilities are illustrated in these sample cases, where setting up different instances of the same application may be required:

1. Organizations operating in different countries, with regional units managed autonomously, where each region needs to implement PAM for multiple instances. Installing separate instances for every region not only adds to the financial and operational burden, but also increases the operations' complexity.

2. Managed service companies with logically separated business units to support different customer operations. To illustrate, Internet Service Provider's CRM, Billing, and BSS systems are managed by IT teams, whereas routers, switches, and backbone systems are supported by other teams. The management of backbone systems can also be further divided into mobile network backbone and fixed network. All these teams, which may be geographically separated and working under different management structures, may require their own dedicated PAM instance for their infrastructure.

Figure 1 — Dedicated PAM for Geographically Dispersed Users

3. Manufacturing companies, with geographically dispersed and autonomously managed production facilities, requiring separate and dedicated PAM instances for every production facility.

4. Companies with a growth strategy based on Mergers and Acquisitions, or holding companies with a large portfolio, may require a PAM solution for each acquired company, or subsidiary.

5. Service providers not only require separate instances to be installed for every customer, but also have to manage incidents across different customer instances, while maintaining separate instances, in line with the agreed upon SLAs for customer retention.

Challenge (continued)

Deploying separate distances for every group of users (business units, different customers) brings up some limitations:

- **Maintenance Complexity:** In case of product changes or upgrades, IT personnel needs to upgrade each application separately, which creates rigidity and inefficiency in managing the application.

- **Scalability:** Using separate instances for every business unit or customer requires additional instance installations with different databases, and re-integration of the external systems already integrated with the existing instances.

- **Lack of Visibility and Control:** Administrators spend significant time and effort to control multiple distributed instances.
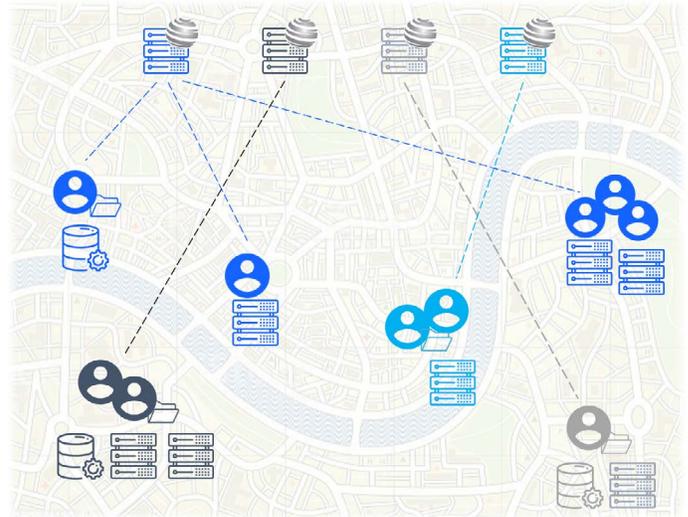

Figure 2 — Dedicated PAM for Each Division/Department

- **Inefficient Use of Resources:** Inefficient use of both human and hardware resources to manage different instances of the same application.
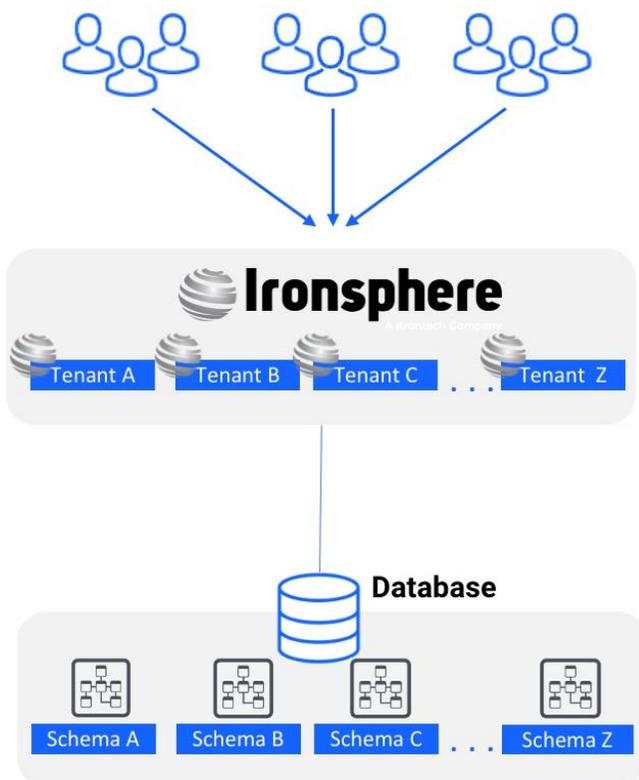
Solution

Figure 3 — Single Instance to Server – Multiple Tenants

Ironsphere, with its multitenant architecture, enables multiple users to share multiple isolated and virtually separated Ironsphere services running on a single instance. Based on this architecture, several groups of users representing different customers, business units or subsidiaries, i.e., tenants, can be created.

Tenants are logically isolated from each other, and each tenant's data remains invisible to other tenants, with a separate schema created on the database for every tenant, ensuring data security.

Every tenant has access to the capabilities offered by a single Ironsphere instance, including the following:

- Unique name and logo
- Users
- Licenses defined by the Host Admin
- Device and Policy Management
- Reports
- Logs
- Audit reports

Tenant Management

The Host Admin is responsible for creating tenants and assigning an administrator to each tenant. Once a tenant is created and a tenant admin assigned, tenant admins can take control and are responsible for tenant management. When required, tenants can also be managed by privileged Host users, if the On behalf of management feature is enabled.

The On behalf of management feature gives Host Admins the flexibility to manage other tenants on their behalf, whenever tenants prefer to have host administrators perform configurations, restore/backup, and other maintenance activities. Data Center providers, for instance, can leverage this capability to provide PAM services, as well as data infrastructure services, and manage access to the servers on behalf of their customers.
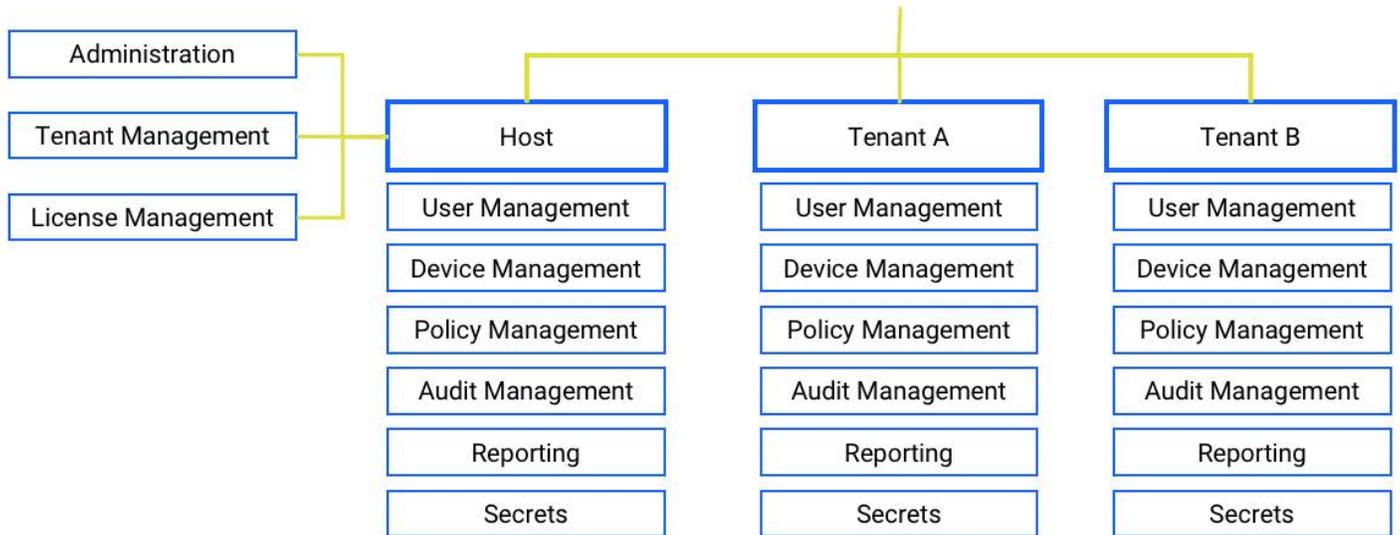

Figure 4 — Tenant Management

Conclusion

Ironsphere's Multitenancy capabilities improve operational efficiency, while enhancing security for organizations. There are various business models where multitenancy can be implemented, so that different business units or customers can get service on a single instance with shared resources.

Sample Case: Multitenancy for Big Organizations

Big organizations can benefit from multitenancy by using a single instance of Ironsphere to serve multiple departments. Each department can manage itself independently, with logical isolation of Ironsphere services, while sharing the same physical infrastructure. Departments can also have their own policies and configurations, independently from other departments.
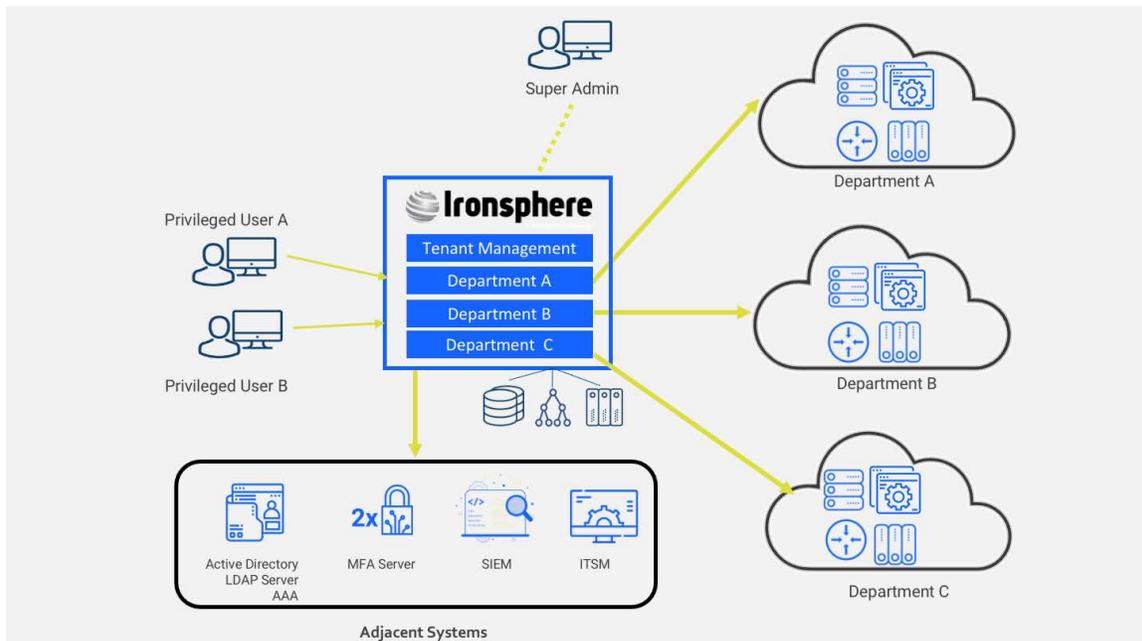
Conclusion (continued)

Figure 5 — Multitenancy for Big Organizations

Benefits:

- Install/maintain a single Ironsphere instance
  for all departments
- Audits can be tracked in a single application
- All IT, Network, Database Management Departments,
  etc., access management needs can be managed
  by a single application, in a single box
- Audit Trails, Logs and Reports are isolated for
  each department
- Single LDAP, SIEM, SMTP integration

Ironsphere's multitenancy architecture is an ideal fit for various business cases, such as MSP/MSSPs, Private PAM as a Service, and Public PAM as a service scenarios.

Multitenancy enables MSPs and MSSPs to host multiple clients effectively, managing their client's needs in a single instance deployment. Rather than creating separate instances for each customer, by configuring each customer infrastructure as a

tenant, MSSPs can save time and resources. Multitenancy gives MSPs/MSSPs the ability to scale their business rapidly, with shorter time-to-market, without the need for additional installations or new resources for every new instance.

Data Center providers can offer Private PAM as a Service to their existing enterprise customers, to track and secure privileged access to their servers/systems at Private Data Centers. Multitenancy will enable Service Providers to support multiple customers within a unified, simplified admin and operations platform, while remaining isolated from each other.

In addition to Private PAM as a Service, multitenancy enables companies to provide PAM as a Service through a multitenant Ironsphere installation on the cloud. Small and Medium size companies can smoothly subscribe to the service, while Service Providers benefit from the easy on-boarding capabilities made available by Ironsphere's multitenant architecture.

Ironsphere
A Krontech Company