HOW-TO GUIDE FOR MIGRATING TO SKYTAP CLOUD
# TABLE OF CONTENTS

**Introduction**

**Planning your migration**
- Define your cloud strategy before migration strategy
- Select an application migration strategy
- Evaluate application workload
- Define your Skytap cloud architecture

**Moving to Skytap Cloud**
- Export images from your datacenter
- Import environments into Skytap Cloud
- Configure your Skytap network
- Working with Skytap templates
- Skytap application firewall and load balancer
- Connecting Skytap Environments
- Importing data
- Operating system licenses
- Creating your cloud security plan
- Application and user Management
- Monitoring Skytap cloud usage
- Disaster Recovery
- Additional resources

**Appendix**
INTRODUCTION

Skytap Cloud is the only public cloud where enterprises can run traditional, mission-critical business applications unchanged, including x86 VMware, AIX and Linux on Power workloads. Skytap Cloud helps you improve business responsiveness by:

- Removing environment contention
- Eliminating configuration drift
- Enabling modern Agile and DevOps practices
- Accelerating the modernization to microservices, containers, and cloud native services.

We’ve seen enterprises achieve success on their cloud modernization journey by using our progressive Infrastructure Modernization, Process Modernization, and Architecture Modernization (IPA) approach, referenced below.

This guide focuses on Infrastructure Modernization, providing a framework based off the extensive experience and insight of Skytap’s professional services team, which helps enterprises, analyze, migrate and run complex, business-critical applications in Skytap Cloud.
Moving to the cloud can be a daunting process given the pressure to migrate and modernize rapidly without jeopardizing the business. The key to success is modernizing iteratively by breaking your journey into realistic, attainable segments.

In our experience, a smooth migration to Skytap Cloud requires strong executive champions and a dedicated cross functional project team, led by a project manager with knowledge of the organization’s processes and procedures. This group should include representatives from the following groups/individuals:

- Business
- Security
- Support
- Enterprise/cloud architects
- Corporate IT
- Cloud administrator(s)
- Application SME’s

Define your cloud strategy

Your organization’s Cloud Strategy provides the foundation for migrating existing applications to the cloud, including application priorities and Key Performance Indicators (KPIs). The Skytap ebook *Considerations when modernizing a traditional applications in a multi-cloud world* is a valuable guide if you’re considering a multi-cloud strategy.

Define business reasons for moving to Skytap Cloud

Establish the reasons for migrating to Skytap Cloud and how you plan to measure success. Focus on long-term business goals and benefits, such as improving release times, gaining new insights or improving quality.

Define migration metrics

Your reason to migrate and migration strategy will drive migration success metrics, which includes availability, resource optimization, cost of infrastructure, and project time.

Evaluate your organization’s readiness

Consider the organizational culture, appetite for change, and skill gaps along with process changes that can be identified and documented upfront. Gartner report: “Align Your Cloud Infrastructure to Your Business Strategy in Four Steps” by Bob Gill provides guidance on where to begin your cloud strategy.

Prioritize applications

Analyze and evaluate your application workload using the evaluation table in the next section, and then create a prioritized list.
Identify one or more typical applications that best represent connections to other resources, access permissions, DNS, load balancers, etc. to run first as a PoC (Proof of Concept) for validating migration in to Skytap Cloud.

**Build stakeholder teams**

Two cross functional teams are vital to migrating successfully: **Governance** and **Delivery**.

The **Governance team** typically doesn’t own the individual migration efforts but is responsible for operating the Skytap Cloud. The Governance team is typically comprised of Corporate IT, Security, Cloud Architect(s), and a Skytap Cloud Admin.

The **Delivery team** is a cross-functional delivery team(s) formed to support the migration of business applications. The Delivery team may vary by application, but should include application owners, SMEs, Architects, Network Engineers, Security, QA, and Corporate IT.

**Build a migration roadmap**

With a plan and teams in place, the next step is to build a migration roadmap that will provide full transparency to the business and application migration teams. The roadmap is also used to track cloud administration activities, application migration, integration, and connections and validations. See the example roadmap timeline at the end of this document.

**Select an application modernization approach**

The **Skytap Guide to Evaluating your Traditional Application Portfolio** provides a framework to evaluate your organizations application portfolio and align a modernization approach that best meets the business need.

Three common migration strategies exist that focus on quickly consolidating or evacuating data centers while making small but necessary architectural or platform changes:

<table>
<thead>
<tr>
<th>Tolerate</th>
<th>Invest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep with minimal to no investment</td>
<td>Lift and extend with some re-factoring likely</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Replace</th>
<th>Redesign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decommission or replaced with new Commercial off the Shelf (COTS) solutions</td>
<td>Has received some modernization; re-architect/re-write cloud native</td>
</tr>
</tbody>
</table>

After migrating to the Skytap Cloud, see **Skytap's guide to application modernization** for additional guidance for modernizing your application development process, including the adoption of agile tools, and different approaches (with example architecture) to Refactor, Re-architect, or Rewrite your traditional applications.
Evaluate application workload

As you evaluate your application portfolio you must define a strategy for each application. Then, identify 2-3 applications as good candidates for a proof of concept to migrate and run in Skytap Cloud.

One application should be a ‘typical’ application representing the range of applications you want to migrate. While this might require more effort than your most basic application, it provides an opportunity to identify and evaluate considerations for a full migration, such as:

- Connections to external resources
- Security profiles
- Access permissions
- Network architecture
- Load balancing and firewall configurations

During this process, you must also assess the application’s complexity, interfaces, authentication methods, data structures, and latency requirements. You should also know its operational requirements, such as service levels, maintenance windows, monitoring, and any backup or disaster recovery requirements.

The template on the next page provides the most common areas to be captured as part of your application migration planning.

This first step is to capture the underlying components that make up the infrastructure that runs the application. This will help you size your environments appropriately in Skytap Cloud.
<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Current App &amp; Infrastructure Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtualization</strong></td>
<td>Ex. VMware, AIX/Linux on Power, Hyper-V</td>
</tr>
<tr>
<td><strong>Current infrastructure/vm size and count</strong></td>
<td>Ex. include os, memory, processor, storage and number of servers/vms with this configuration. List for each component of your applications’ infrastructure</td>
</tr>
<tr>
<td><strong>Containers</strong></td>
<td>Ex. Docker</td>
</tr>
<tr>
<td><strong>Database</strong></td>
<td>Ex. DB2, SQL, Oracle v.x, Oracle RAC, MySQL, MongoDB</td>
</tr>
<tr>
<td><strong>Packaged Software used</strong></td>
<td>Ex. SAP, EPIC, Websphere</td>
</tr>
<tr>
<td><strong>SSO</strong></td>
<td>Ex. Okta, Ping, Azure AD, Salesforce</td>
</tr>
<tr>
<td><strong>Synchronization to on-premise identity store</strong></td>
<td>Ex. Active Directory, LDAP</td>
</tr>
<tr>
<td><strong>External network connections &amp; locations to Skytap</strong></td>
<td>Ex. secure, dedicated, direct high bandwidth connection - West Secure, standard connection - East</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>Ex. Isolated or extension of on-prem, layer2, layer3</td>
</tr>
<tr>
<td><strong>Load balancer</strong></td>
<td>Ex. virtualized F5</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>Ex. F5</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Ex. Splunk</td>
</tr>
<tr>
<td><strong>Clustered</strong></td>
<td>Ex. Yes / No</td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td>Ex. Yes / No. SLA</td>
</tr>
<tr>
<td><strong>Geolocation of application</strong></td>
<td>Ex. North America Central, London, Sydney</td>
</tr>
<tr>
<td><strong>Storage used</strong></td>
<td>Ex. 30GB</td>
</tr>
</tbody>
</table>
Define your Skytap Cloud architecture

With an understanding of your application Cloud portfolio in its current state, your next step is to define the landing zone in Skytap Cloud. This is a good time to engage with Skytap’s professional services team, who can provide you with additional guidance and best practices by embedding themselves in your migration team.

Your target landing zone in Skytap Cloud includes the technical foundation for the workloads you plan to migrate and the environments that will be managed and accessed.

Laying the technical foundation in Skytap Cloud is driven by the network architecture. You must define the operating environment for your applications and include network configuration, external connections through VPN and Skytap’s dedicated Private Network Connection, and components such as virtualized load balancers and firewalls.

A workflow model is used to describe how users access and update applications running in Skytap Cloud. The model should also describe the integration with CI/CD and the monitoring tools (and the required permissions) to clone, copy and delete within Skytap Cloud.

Document and validate your architecture

Documenting your Skytap Cloud architecture is important as it provides the blueprint for teams that will perform the migration tasks that are outlined in the next section of this guide.

Begin with your current state architecture and workflow documentation as a guide for the architecture requirements for the target landing zone in Skytap Cloud, focus on maintaining as close to current state as possible.

1. Landing zone in Skytap Cloud
   A. Covers current state assessment and development of target state network architecture and implementation steps, Security profile, dev tools integration and ecosystem details

2. Target state Migration and Implementation planning
   A. Includes plan for application migration, target state operational model, on-boarding of teams, and secure connectivity implementation

Before migrating to Skytap Cloud, validate your Skytap Cloud architecture with application SMEs from your delivery team and ensure that you are meeting your business objectives.

This stage provides an opportunity to also document any desired future enhancements—for example, introducing automation and modernizing applications for microservices and containers.

See Skytap’s Practical Guide to Using Skytap Cloud, Containers & CI/CD Tools for Modernizing Traditional Applications for a vision to common future states for enterprises adopting modern tools and services in Skytap Cloud.
MOVING TO
SKY TAP CLOUD

Having assessed, prioritized and selected a migration approach for the applications in your organization, the next steps will be migrating applications, configuring environments, and providing your users access to Skytap Cloud.

Export images from your datacenter

You can import the following images into Skytap Cloud:

- OVA
- OVF
- VMX
- vApp
- IBM Power System VMs

Non-VMware virtual machines, like Xen and Hyper-V, require conversion before they can be imported. See Converting Non-VMware VMs in Skytap Help & Documentation.

Best practices for exporting VM images

Before exporting a VM, make sure the VM is configured optimally to be imported into Skytap Cloud:

- Ensure the VM has a local administrator account.
- Remove snapshots or linked copies from VM files.
- Leave one IDE interface available for Skytap Cloud to add a CD/DVD drive (to load ISOs).
- Configure VMs to use DHCP networking. Skytap Cloud creates automatic networking for your environment.
- Power off each VM in the import job.

Import environments into Skytap Cloud

Skytap provides several options for importing pre-configured VMs, vApps, and LPARs in to Skytap Cloud as environments.

Where possible we recommend using vApps, because the import process will retain OS and application settings along with network settings. Further instructions for using our migration tools can be found in the Skytap Help Center.
Basic importing through Skytap
You can access the Skytap basic import feature through the Skytap Cloud Environments page. Note that administrators can also enable this self-service option for end users.

Basic import is best for importing a small number of lightweight VMs that don’t require validation.

Importing with the Skytap Advanced Import Appliance
If you need to streamline a large-scale migration of VMs, or if you need to import recurring jobs, we recommend using the Skytap Advanced Import Appliance.

The Skytap Advanced Import Appliance scans a network location for VMs and IBM Power System LPARs. It then validates the VM files and manages the migration to Skytap Cloud.

The Skytap Advanced Import Appliance can also be used as part of evaluating your application portfolio, after which you can let the automated queueing manage the migration to Skytap Cloud.

Importing with the Skytap Advanced Import Service
If you need to import large volumes of data with high privacy and security requirements, you can use the Skytap-assisted Advanced Import Service to physically ship VMs on a hard disk from your data center to Skytap’s data center.

Configure your Skytap network
Skytap Cloud network management features were designed to remove the complexity of environment networking, connecting environments and through environment network isolation, enable multiple, complete replicas of your application environments to run without IP address conflicts.

Designing Skytap network controls
The first consideration when thinking about Skytap Cloud network design are the controls required for Skytap environments, including public access to and from the internet.

Skytap environments can have full Internet egress and ingress, or more restrictive controls that can route traffic via VPN through your corporate network. Skytap controls can also create a virtualized firewall in the Skytap environment.

These controls can also be applied to connections between existing on-premise infrastructure and other hyper-scale cloud services and resources.

A second consideration is whether there are components that can’t be replicated directly into Skytap Cloud, such as physical firewalls or load balancers, that may need to be replaced with virtual equivalents. This affects decisions around what DNS, if any, is required and the IP range that you want to use.
Configuring connectivity

Under Skytap Network Settings, you can create **VPNs** available to all Skytap environments as a configuration option.

Skytap’s **Private Network Connection (PNC)** creates a dedicated, low latency, point-to-point network connection from your Skytap Cloud region to an on-premise data center or other cloud instance(s). This, in turn, enables fast and reliable network performance for high transaction applications, and/or a fast migration to Skytap Cloud.

Your current corporate network is likely to have a firewall managing network traffic for VPN and PNC connections to be able to access on-premise resources, and similarly for internal corporate traffic to access Skytap. Your corporate firewall may need to be configured to allow specific port and IP traffic to and from Skytap.

Configuring environment network settings

Skytap provides **automatic networking** services that provide IP addresses, DHCP and DNS services, outbound public connectivity and prevents IP address conflicts between VMs, which persists when end users copy and clone environments.

You can configure the default automatic network configuration for each environment in the **Skytap network settings** page, where you can configure the following:

- Network IP address range
- Subnet and default gateway
- Domain
- DNS, ICNR & NAT (see below).

You can also manually manage your network configuration through **network settings**, where Skytap Cloud provides a virtual network (vlan) and allows you to manage your own IP addressing and subnet via static IP assignment or, more commonly, when running your own DHCP and DNS server in the environment.

See Skytap’s help topic **What is the difference between automatic and manual networks?** for more information.

Make Skytap environments available externally to non-Skytap users

Environments and VMs can also be made accessible to external, non-Skytap users through the methods below.

<table>
<thead>
<tr>
<th>Sharing Portals</th>
<th>Sharing portals provide browser-based access to VMs and environments for non Skytap Cloud account holders, like external contractors and partners.</th>
<th>Password &amp; time-controlled access to Skytap environments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP</td>
<td>A public IP address allows unrestricted access to all ports on the attached VM. This provides easy access but comes with a greater security</td>
<td>Exposes all network ports on a VM accessible IP address. Only available with Skytap automatic network.</td>
</tr>
<tr>
<td>Published services</td>
<td>Published services are commonly used to access a VM via SSH or direct RDP, or to access web or application services running on a VM.</td>
<td>Network level access to VM's Note: VM firewall rules may need to be edited to allow traffic over the port you are publishing.</td>
</tr>
</tbody>
</table>
Working with Skytap templates

The Skytap template library includes public sysprepped operating system templates, personal templates that end users can save for their own use, and company templates available across your organization.

As organizations migrate to Skytap Cloud, common applications are identified as candidates to be added as templates.

These environments are then:

1. Prepared as ‘golden templates’ by IT and application owners.
2. Reviewed by security.
3. Validated in Skytap cloud and then published.

Corporate IT and security teams sometimes worry that moving to the cloud sacrifices control of their environment through the introduction of unapproved applications. Although audits and reviews won’t disappear entirely in a Skytap Cloud environment, it is easier for IT and security teams to proactively pre-approve environments that are made available across organizations.

Skytap application firewall and load

Internet-facing applications running in a Skytap Cloud environment commonly require a virtual firewall appliance to control access, reduce vulnerabilities from inbound traffic, and/or restrict outbound traffic.

If you are migrating from an on-premise data center where applications use physical load balancing, you can add a virtual load balancer to your Skytap environment.

Skytap Cloud supports any virtual appliance that VMware supports on x86 architecture. In addition, the Skytap Cloud public template library includes the Radware Alteon virtual appliance (VA) to provide functionality identical to Alteon physical ADC devices.

Connecting Skytap Environments

By default, Skytap environments are isolated from each other, which enables multiple clones of an environment (down to layer 2 network) to run in parallel without conflict. Skytap Inter-Configuration Network Routing (ICNR) and Network Address Translation (NAT) enables communication between Skytap environments.

When configuring a Skytap environment network two additional settings are provided that enable ICNR between environments:

- Visible to other networks: This makes the environment visible to other environments, the first step in implementing Skytap ICNR, most common in larger shared environments.
• Apply NAT for connecting networks: If you are leveraging Skytap Automatic Networks you can enable Network Address Translation (NAT) to prevent IP address overlap between connected environments.

Complete the configuration between the two environments from the **network settings** page by selecting ‘connect to a network’. Here you will see all environments that are visible to other networks.

**Note:** Importing vApps significantly reduces the network configuration required as network configuration is retained in the vApp.

## Importing data

Typically data is imported with VM’s and Skytap Cloud provides a web-based file ‘**Assets**’ repository that you can access from your computer and your Skytap Cloud VMs. This repository can be used to host ISO images for VMs along with other files or VMs that project teams may require. Items in the asset repository can also be shared with users through projects.

Be sure to validate the dataset after it is imported, and choose an approach for incremental data refreshes from the following options:

- Restoring the database
- Dropping the existing database and restoring a backup from the primary database
- Refreshing the database, whereby the database remains, and database changes are replicated.

One additional consideration is whether you need to obfuscate data when moving it between production, development, and test environments. Make sure your test plan covers this and can be applied to operations that run in Skytap Cloud.

## Supported operating systems

Skytap Cloud supports the following popular operating systems:

<table>
<thead>
<tr>
<th>X86 operating systems</th>
<th>Power operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>AIX*</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>Ubuntu Server</td>
</tr>
<tr>
<td>CentOS</td>
<td>SUSE Enterprise Server</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
</tr>
</tbody>
</table>

* Minimum supported AIX versions available at [help.skytap.com/OS_Support.html](http://help.skytap.com/OS_Support.html)
Operating system licenses

Skytap provides VMs with pre-installed operating systems through Skytap Cloud Public templates, generally these VMs do not include any product, or licensing keys, speak to your Skytap account representative for guidance and facilitating acquiring appropriate licenses.

Skytap can provide you Windows SPLA & Red Hat Enterprise Linux (RHEL) licensing, and for those running Oracle we have a white paper on Licensing Oracle in Skytap Cloud.

Creating your cloud security plan

It is a common misconception that moving to the cloud is less secure than on-premise solutions. But with the right processes and precautions, the cloud can be even more secure than on-premise solutions.

Many common IT security practices still apply to cloud-based operations, but as you move to introduce automation and native cloud-based approaches, then you may need to introduce additional security and changes to how existing security operations teams operate.

Key considerations to include in your Cloud Security Plan:

- The type of workloads you plan to run in Skytap and subsequently what tools are necessary
- Certifications, accreditations, and industry standards, such as SOC2, HIPPA, GDPR & FedRAMP
- Which applications and data can easily be moved to the cloud.
- Governance
- Security processes - with the introduction of automation, a move to pre-accreditation of cloud services and environments is common. The concept of golden environments.
- Authentication and Authorization mechanisms, such as SSO, IP-based restrictions, and access control lists.
**Application and user Management**

Skytap Cloud administrators have access to an extra section of the navigation menu, called Admin. The Admin section contains global settings, customization options, reporting, policy management and ability to add/remove new user accounts.

See Skytap’s [Administrator Guide](#) to get started managing Skytap Cloud.

When setting up Skytap Cloud there are several considerations and activities to plan before importing or providing user access, these include:

**Single Sign-on**

Skytap Cloud supports federated authentication via SAML 2.0 single sign-on (SSO) to enable users to automatically log into Skytap Cloud after being authenticated by an Identity Provider (IdP), such as Active Directory (AD) or LDAP.

See [Using Single Sign-on (SSO)](#) in Skytap help for more information.

**Integrating Active Directory**

For Microsoft AD integration, there are two approaches:

**AD Managed Environments:** Users are bound to an on-premises AD controller, essentially making Skytap an extension of the on-premise network. This method provides familiar work patterns and an easy extension of existing security models. A key consideration when cloning environments is that each new clone will require a new hostname and may require a new SID.

**Self-Contained Environments:** VMs are managed entirely by Skytap Cloud users. Self-contained environments provide the most flexibility of use but will be limited to what external and on-premise resources can be used from within the environment. Servers and services should be moved into Skytap and contained within the Skytap application environment with limited access to external services. This approach best leverages Skytap Cloud, enabling self-service deployment of applications, full cloning of environments and best supports adopting automation workflows.

For more information, see [Best practices for running a Windows domain in Skytap](#).

**Managing Skytap users**

Use the admin section in Skytap Cloud to add and manage accounts. Bulk actions such as creating many users can be automated through the Skytap Cloud REST API. Skytap has a sample Python script and CSV in the [Skytap GitHub](#) repository to assist.

See [Managing users and permissions](#) in Skytap help for more information.

**Skytap user roles**

When you create a user, you assign one of four user roles:

- **Restricted:** This role is best for users who need tightly-controlled access to a limited number of resources.
- **Standard:** The standard role for typical users.
- **User Manager:** This role is best for users who need to manage and organize users and groups but don’t need full administrator capabilities.
- **Administrator:** Best for trusted users in your organization who need to manage users, resources, and account-wide settings.

See the table on the following page for a complete breakdown of user roles and permissions.
Skytap user role permissions table

<table>
<thead>
<tr>
<th>Restricted</th>
<th>Standard</th>
<th>User Manager</th>
<th>Administrator</th>
<th>Can do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Access shared project resources</td>
</tr>
<tr>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Create and own projects</td>
</tr>
<tr>
<td>**</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Create environments, templates, and assets</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Create and edit users and groups</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Delete groups</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Create and edit departments</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Delete users</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Create and edit account-wide settings (password policies, access policies, usage limits, etc.)</td>
</tr>
<tr>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>Edit and delete environments, templates, and assets owned by all users in the account.</td>
</tr>
</tbody>
</table>

* A restricted user can’t create a project, but another user can make a restricted user a project owner.
** Restricted users have limited permission to create environments.

Additional permissions can be applied at a user level for access to VPN, assets, templates, and provide the ability to import. For more information, see Understanding project roles.

Quota allocation and cost management

Skytap monitors four types of usage:

- Storage
- SVM hours
- Concurrent VMs
- Concurrent SVMs

**Note:** If your subscription includes Power Systems SVM hours, concurrent SVMs are tracked separately for x86 and Power VMs.

You can set limits for each type of usage globally, by region, by department, or by individual user. If multiple limits for the same type of usage are established—for example, a regional storage limit, a department storage limit, and a user storage limit—then the user’s usage is halted when any of those limits are met.

Environment Controls

You can manage resource usage in Skytap environments by scheduling environment operating times and power options to auto-suspend and auto shut-down environments if they have been inactive for a period of time.

Usage restrictions

Skytap Cloud automatically prevents users from performing actions that would exceed a limit (such as creating a template or running VMs).
When a limit is reached, the user, department, or account will be affected as follows:

- SVM Hours limit reached: All running VMs are suspended. You can’t use more SVM Hours unless you increase the user, department, or account limit.
- SVM or VM limit reached: No more VMs can be started. Stop running VMs to release SVMs and VMs and allow more to be started.
- Storage limit reached: No more templates or environments may be created. Delete templates or environments to allow more to be created.

See Setting usage limits in Skytap help for more information.

**Monitoring Skytap cloud usage**

Skytap Admins can use the admin console to add and manage users, apply resource quotas, set alerts, and monitor Skytap cloud usage across regions.

Skytap Cloud uses different controls than other public clouds for managing cloud resources. Quotas define how many system resources an end user can use, enabling tighter management of cloud costs and VM sprawl. You can also set notifications to inform the user when a limit is reached or when a VM has been left running for an extended period.

**Disaster Recovery**

Skytap Cloud supports multiple disaster recovery solutions. Available solutions include cold and warm off-site disaster recovery for your applications running in your on-premise data center, as well as disaster recovery to an alternate region for applications running in Skytap Cloud.

We have provided reference architecture for cold & warm DR scenarios:

- Disaster Recovery Reference Architectures
- On-Prem to Skytap – Cold Recovery
- On-Prem to Skytap – Warm Recovery
- Skytap Region to Skytap Region – Cold Recovery
- Skytap Region to Skytap Region – Warm Recovery

Organizations will commonly bring their own third-party monitoring tools like Splunk or Nagios to monitor applications, network and services. See Splunk’s Installation and configuration overview for the Splunk Add-on for VMware.
Additional resources

Skytap is invested in helping our customers achieve their business goals. Our experienced team of consultants, engineers and architects can assist in current state SDLC and application portfolio evaluation, architecting, onboarding, and implementing your Skytap Cloud solution.

For more information on how Skytap can help you with your modernization journey, see the following resources:

- Whitepapers and Market Insights
- Skytap Partner Solutions
- Skytap Academy
- Skytap Product Tour
- Modernizing in a Multi-Cloud world
- Guide to application modernization
- AIX Migration guide
- Licensing Oracle in Skytap

Appendix

Skytap Modernization Roadmap example
This Is a Cloud Adoption Framework

1. Build Skills and Assess Applications
2. Select Cloud Providers and Services
3. Architect Cloud Services and Mitigate Risks
4. Estimate the Bill and Establish Governance
5. Provision and Automate Cloud Services
6. Operate Cloud Environments at Scale

Gartner: Align Your Cloud Infrastructure to Your Business Strategy in Four Steps

Skytap Cloud’s Infrastructure Modernization, Process Modernization, and Architecture Modernization (IPA) approach

Transform Over Time, Not Overnight
Modernization with Skytap Cloud

Infrastructure Modernization
Adopt cloud infrastructure to eliminate SDLC constraints

Process Modernization
Introduce agile & DevOps processes along with CI/CD automation

Architecture Modernization
Accelerate innovation using new cloud native architectures and services