Small-to-medium enterprise: Multicloud evolution

02/11/2019 • 4 minutes to read • Contributors

In this article

This article evolves the narrative by adding controls for multicloud adoption.

Evolution of the narrative

Microsoft recognizes that customers are adopting multiple clouds for specific purposes. The fictional customer in this journey is no exception. In parallel to the Azure adoption journey, the business success has led to the acquisition of a small, but complementary business. That business is running all of their IT operations on a different cloud provider.

This article describes how things change when integrating the new organization. For purposes of the narrative, we assume this company has completed each of the governance evolutions outlined in this customer journey.

Evolution of the current state

In the previous phase of this narrative, the company had begun actively pushing production applications to the cloud through CI/CD pipelines.

Since then, some things have changed that will affect governance:

- Identity is controlled by an on-premises instance of Active Directory. Hybrid identity is facilitated through replication to Azure Active Directory.
- IT Operations or Cloud Operations are largely managed by Azure Monitor and related automations.
- Disaster Recovery / Business Continuity is controlled by Azure Vault instances.
- Azure Security Center is used to monitor security violations and attacks.
- Azure Security Center and Azure Monitor are both used to monitor governance of the cloud.
- Azure Blueprints, Azure Policy, and Azure management groups are used to automate compliance with policy.

Evolution of the future state

The goal is to integrate the acquisition company into existing operations wherever possible.

Evolution of tangible risks

Business acquisition cost: Acquisition of the new business is estimated to be profitable in approximately five years. Because of the slow rate of return, the board wants to control acquisition costs, as much as possible. There is a risk of cost control and technical integration conflicting with one another.

This business risk can be expanded into a few technical risks:

- Cloud migration might produce additional acquisition costs.
- The new environment might not be properly governed, which could result in policy violations.

Evolution of the policy statements

The following changes to policy will help remediate the new risks and guide implementation.

1. All assets in a secondary cloud must be monitored through existing operational management and security monitoring tools.
2. All Organization Units must be integrated into the existing identity provider.
3. The primary identity provider should govern authentication to assets in the secondary cloud.

Evolution of the best practices

This section of the article will evolve the governance MVP design to include new Azure policies and an implementation of Azure Cost Management. Together, these two design changes will fulfill the new corporate policy statements.

1. Connect the networks. This step is executed by the Networking and IT Security teams, and supported by the Cloud Governance team. Adding a connection from the MPLS/leased-line provider to the new cloud will integrate networks. Adding routing tables and firewall configurations will control access and traffic between the environments.
2. Consolidate identity providers. Depending on the workloads being hosted in the secondary cloud, there are a variety of options to identity provider consolidation. The following are a few examples:
   a. For applications that authenticate using OAuth 2, users from Active Directory in the secondary cloud can simply be replicated to the existing Azure AD tenant. This ensures all users can be authenticated in the tenant.
   b. At the other extreme, federation allows OUs to flow into Active Directory on-premises, then into the Azure AD instance.
3. Add assets to Azure Site Recovery.
   a. Azure Site Recovery was designed from the beginning as a hybrid or multicloud tool.
   b. VMs in the secondary cloud might be able to be protected by the same Azure Site Recovery processes used to protect on-premises assets.
4. Add assets to Azure Cost Management
   a. Azure Cost Management was designed from the beginning as a multicloud tool.
   b. Virtual machines in the secondary cloud may be compatible with Azure Cost Management for some cloud providers. Additional costs may apply.
5. Add assets to Azure Monitor.
   a. Azure Monitor was designed as a hybrid cloud tool from inception.
   b. Virtual machines in the secondary cloud may be compatible with Azure Monitor agents, allowing them to be included in Azure Monitor for operational monitoring.
6. Governance enforcement tools:
   a. Governance enforcement is cloud-specific.
   b. The corporate policies established in the governance journey are not cloud-specific. While the implementation may vary from cloud to cloud, the policies can be applied to the secondary provider.

As multicloud adoption grows, the design evolution above will continue to mature.

Conclusion

This series of articles outlined the evolution of governance best practices, aligned with the experiences of this fictional company. By starting small, but with the right foundation, the company could move quickly and yet still apply the right amount of governance at the right time. The MVP by itself did not protect the customer. Instead, it created the foundation to manage risks and add protections. From there, layers of governance were applied to remediate tangible risks. The exact journey presented here won't align 100% with the experiences of any reader. Rather, it serves as a

pattern for incremental governance. The reader is advised to mold these best practices to fit their own unique constraints and governance requirements.