Large enterprise: Multicloud evolution

02/11/2019 • 3 minutes to read • Contributors

In this article

Evolution of the narrative

Microsoft recognizes that customers are adopting multiple clouds for specific purposes. The fictional company 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 to implement cost controls and cost monitoring, as cloud spending becomes part of the company's regular operating expenses.

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 management groups are used to automate compliance to 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

- There is risk of cloud migration producing additional acquisition costs.
- There is also a risk of the new environment not being properly governed or resulting 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 organizational 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. Executed by Networking and IT Security, supported by governance.
   a. Adding a connection from the MPLS or 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 in the Active Directory in the secondary cloud could simply be replicated to the existing Azure AD tenant.
   b. On the other extreme, federation between the two on-premises identity providers, would allow users from the new Active Directory domains to be replicated to Azure.
3. Add assets to Azure Site Recovery.
   a. Azure Site Recovery was built as a hybrid and multicloud tool from the beginning.
   b. Virtual machines 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 built as a multicloud tool from the beginning.
   b. Virtual machines in the secondary cloud might be compatible with Azure Cost Management for some cloud providers. Additional costs may apply.
5. Add assets to Azure Monitor.
   a. Azure Monitor was built as a hybrid cloud tool from the beginning.
   b. Virtual machines in the secondary cloud might 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 policy statements can be applied to the secondary provider.

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

Next steps

In many large enterprises, the Five Disciplines of Cloud Governance can be blockers to adoption. The next article has some additional thoughts on making governance a team sport to help ensure long-term success in the cloud.

Multiple layers of governance