Small-to-medium enterprise: Resource Consistency evolution

02/11/2019 • 6 minutes to read • Contributors

In this article

This article evolves the narrative by adding Resource Consistency controls to support mission-critical apps.

Evolution of the narrative

New customer experiences, new prediction tools, and migrated infrastructure continue to progress. The business is now ready to begin using those assets in a production capacity.

Evolution of the current state

In the previous phase of this narrative, the application development and BI teams were nearly ready to integrate customer and financial data into production workloads. The IT team was in the process of retiring the DR datacenter.

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

- IT has retired 100% of the DR datacenter, ahead of schedule. In the process, a set of assets in the Production datacenter were identified as cloud migration candidates.
- The application development teams are now ready for production traffic.
- The BI team is ready to feed predictions and insights back into operation systems in the Production datacenter.

Evolution of the future state

Before using Azure deployments in production business processes, cloud operations must mature. In conjunction, an additional governance evolution is required to ensure assets can be operated properly.

The changes to current and future state expose new risks that will require new policy statements.

Evolution of tangible risks

Business interruption: There is an inherent risk of any new platform causing interruptions to mission-critical business processes. The IT Operations team and the teams executing on various cloud adoptions are relatively inexperienced with cloud operations. This increases the risk of interruption and must be remediated and governed.

This business risk can be expanded into several technical risks:

- External intrusion or denial of service attacks might cause a business interruption.
- Mission-critical assets may not be properly discovered, and therefore might not be properly operated.
- Undiscovered or mislabeled assets might not be supported by existing operational management processes.

- The configuration of deployed assets may not meet performance expectations.
- Logging might not be properly recorded and centralized to allow for remediation of performance issues.
- Recovery policies may fail or take longer than expected.
- Inconsistent deployment processes might result in security gaps that could lead to data leaks or interruptions.
- Configuration drift or missed patches might result in unintended security gaps that could lead to data leaks or interruptions.
- Configuration might not enforce the requirements of defined SLAs or committed recovery requirements.
- Deployed operating systems or applications might fail to meet hardening requirements.
- With so many teams working in the cloud, there is a risk of inconsistency.

Evolution of the policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but adopting these policies may be easier than it appears.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the Cloud Governance team and the application owner before deployment to the cloud.
2. Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
3. Governance tooling must audit and enforce network configuration requirements defined by the Security Management team.
4. Governance tooling must validate that all assets related to mission-critical apps or protected data are included in monitoring for resource depletion and optimization.
5. Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
6. Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.
7. Governance tooling must limit virtual machine deployments to approved images only.
8. Governance tooling must enforce that automatic updates are prevented on all deployed assets that support mission-critical applications. Violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT Operations.
9. Governance tooling must validate tagging related to cost, criticality, SLA, application, and data classification. All values must align to predefined values managed by the governance team.
10. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
11. Trends and exploits that could affect cloud deployments should be reviewed regularly by the Security team to provide updates to security management tooling used in the cloud.
12. Before release into production, all mission-critical apps and protected data must be added to the designated operational monitoring solution. Assets that cannot be discovered by the chosen IT operations tooling, cannot be released for production use. Any changes required to make the assets discoverable must be made to the relevant deployment processes to ensure assets will be discoverable in future deployments.
13. When discovered, operational management teams will size assets, to ensure that assets meet performance requirements.
14. Deployment tooling must be approved by the Cloud Governance team to ensure ongoing governance of deployed assets.
15. Deployment scripts must be maintained in a central repository accessible by the Cloud Governance team for periodic review and auditing.
16. Governance review processes must validate that deployed assets are properly configured in alignment with SLA and recovery requirements.

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. The Cloud Operations team will define operational monitoring tooling and automated remediation tooling. The Cloud Governance team will support those discovery processes. In this use case, the Cloud Operations team chose Azure Monitor as the primary tool for monitoring mission-critical applications.
2. Create a repository in Azure DevOps to store and version all relevant Resource Manager templates and scripted configurations.
3. Azure Vault implementation:
    a. Define and deploy Azure Vault for backup and recovery processes.
    b. Create a Resource Manager template for creation of a vault in each subscription.
4. Update Azure Policy for all subscriptions:
    a. Audit and enforce criticality and data classification across all subscriptions to identify any subscriptions with mission-critical assets.
    b. Audit and enforce the use of approved images only.
5. Azure Monitor implementation:
    a. Once a mission-critical subscription is identified, create an Azure Monitor workspace using PowerShell. This is a predeployment process.
    b. During deployment testing, the Cloud Operations team deploys the necessary agents and tests discovery.
6. Update Azure Policy for all subscriptions that contain mission-critical applications.
    a. Audit and enforce the application of an NSG to all NICs and subnets. Networking and IT Security define the NSG.
    b. Audit and enforce the use of approved network subnets and VNets for each network interface.
    c. Audit and enforce the limitation of user-defined routing tables.
    d. Audit and enforce deployment of Azure Monitor agents for all virtual machines.
    e. Audit and enforce that Azure Vault exists in the subscription.
7. Firewall configuration:
    a. Identify a configuration of Azure Firewall that meets security requirements. Alternatively, identify a third-party appliance that is compatible with Azure.
    b. Create a Resource Manager template to deploy the firewall with required configurations.
8. Azure blueprint:
    a. Create a new Azure blueprint named `protected-data`.
    b. Add the firewall and Azure Vault templates to the blueprint.
    c. Add the new policies for protected data subscriptions.
    d. Publish the blueprint to any management group intended to host mission-critical applications.
    e. Apply the new blueprint to each affected subscription as well as existing blueprints.

Conclusion

These additional processes and changes to the governance MVP help remediate many of the risks associated with resource governance. Together they add recovery, sizing, and monitoring controls that empower cloud-aware operations.

Next steps

As cloud adoption continues to evolve and deliver additional business value, risks and cloud governance needs will also evolve. For the fictional company in this journey, the next trigger is when the scale of deployment exceeds 100 assets to the cloud or monthly spending exceeds $1,000 per month. At this point, the Cloud Governance team adds Cost Management controls.

Cost Management evolution