Resource Consistency metrics, indicators, and risk tolerance

02/11/2019 • 5 minutes to read • Contributors

In this article

Metrics
Risk tolerance indicators
Next steps

This article is intended to help you quantify business risk tolerance as it relates to Resource Consistency. Defining metrics and indicators helps you create a business case for making an investment in maturing the Resource Consistency discipline.

Metrics

The Resource Consistency discipline focuses on addressing risks related to the operational management of your cloud deployments. As part of your risk analysis you'll want to gather data related to your IT operations to determine how much risk you face, and how important investment in Resource Consistency governance is to your planned cloud deployments.

Every organization has different operational scenarios, but the following items represent useful examples of the metrics you should gather when evaluating risk tolerance within the Resource Consistency discipline:

- **Cloud assets.** Total number of cloud-deployed resources.
- **Untagged resources.** Number of resources without required accounting, business impact, or organizational tags.
- **Underused assets.** Number of resources where memory, CPU, or network capabilities are all consistently underutilized.
- **Resource depletion.** Number of resources where memory, CPU, or network capabilities are exhausted by load.
- **Resource age.** Time since resource was last deployed or modified.
- **VMs in critical condition.** Number of deployed VMs where one or more critical issues are detected which need to be addressed in order to restore normal functionality.
- **Alerts by severity.** Total number of alerts on a deployed asset, broken down by severity.
- **Unhealthy subnet links.** Number of resources with network connectivity issues.
- **Unhealthy service endpoints.** Number of issues with external network endpoints.
- **Cloud provider service health incidents.** Number of disruptions or performance incidents caused by the cloud provider.
- **Service level agreements.** This can include both Microsoft’s commitments for uptime and connectivity of Azure services, as well as commitments made by the business to its external and internal customers.
- **Service availability.** Percentage of actual uptime cloud-hosted workloads compared to the expected uptime.
- **Recovery time objective (RTO).** The maximum acceptable time that an application can be unavailable after an incident.
- **Recovery point objective (RPO).** The maximum duration of data loss that is acceptable during a disaster. For example, if you store data in a single database, with no replication to other databases, and perform hourly backups, you could lose up to an hour of data.
- **Mean time to recover (MTTR).** The average time required to restore a component after a failure.
- **Mean time between failures (MTBF).** The duration that a component can reasonably expect to run between outages. This metric can help you calculate how often a service will become unavailable.
- **Backup health.** Number of backups actively being synchronized.

- **Recovery health.** Number of recovery operations successfully performed.

Risk tolerance indicators

Cloud platforms offer a baseline set of features that allow deployment teams to effectively manage small deployments without extensive additional planning or processes. As a result, small Dev/Test or experimental first workloads that include a relatively small amount of cloud-based assets represent low level of risk, and will likely not need much in the way of a formal Resource Consistency policy.

However, as the size of your cloud estate grows the complexity of managing your assets becomes significantly more difficult. With more assets on the cloud, the ability identify ownership of resources and control resource useful becomes critical to minimizing risks. As more mission-critical workloads are deployed to the cloud, service uptime becomes more critical, and tolerance for service disruption potential cost overruns diminishes rapidly.

In the early stages of cloud adoption, work with your IT operations team and business stakeholders to identify business risks related to Resource Consistency, then determine an acceptable baseline for risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to remediate these risks. The following are a few examples of how operational metrics, such as those discussed above, can justify an increased investment in the Resource Consistency discipline.

- **Tagging and naming trigger.** A company with more than *x* resources lacking required tagging information or not obeying naming standards should consider investing in the Resource Consistency discipline to help refine these standards and ensure consistent application of them to cloud-deployed assets.
- **Overprovisioned resources trigger.** If a company has more than *x%* of assets regularly using small amounts of their available memory, CPU, or network capabilities, investment in the Resource Consistency discipline is suggested to help optimize resources usage for these items.
- **Underprovisioned resources trigger.** If a company has more than *x%* of assets regularly exhausting most of their available memory, CPU, or network capabilities, investment in the Resource Consistency discipline is suggested to help ensure these assets have the resources necessary to prevent service interruptions.
- **Resource age trigger.** A company with more than *x* resources that have not been updated in over *y* months could benefit from investment in the Resource Consistency discipline aimed at ensuring active resources are patched and healthy, while retiring obsolete or otherwise unused assets.
- **Service-level agreement trigger.** A company that cannot meet its service-level agreements to its external customers or internal partners should invest in the Deployment Acceleration discipline to reduce system downtime.
- **Recovery time triggers.** If a company exceeds the required thresholds for recovery time following a system failure, it should invest in improving its Deployment Acceleration discipline and systems design to reduce or eliminate failures or the effect of individual component downtime.
- **VM health trigger.** A company that has more than *x%* of VMs experiencing a critical health issue should invest in the Resource Consistency discipline to identify issues and improve VM stability.
- **Network health trigger.** A company that has more than *x%* of network subnets or endpoints experiencing connectivity issues should invest in the Resource Consistency discipline to identify and resolve network issues.
- **Backup coverage trigger.** A company with *x%* of mission-critical assets without up-to-date backups in place would benefit from an increased investment in the Resource Consistency discipline to ensure a consistent backup strategy.
- **Backup health trigger.** A company experiencing more than *x%* failure of restore operations should invest in the Resource Consistency discipline to identify problems with backup and ensure important resources are protected.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Resource Consistency discipline will be specific to your organization, but the examples above should serve as a useful base for discussion within your Cloud Governance team.

Next steps

Using the Cloud Management template, document metrics and tolerance indicators that align to the current cloud adoption plan.

Building on risks and tolerance, establish a process for governing and communicating Resource Consistency policy adherence.

Establish policy compliance processes