AWS Environment Management

Best Practices Checklist

A WHITEPAPER BY

[deft]

v21.8

Meet Deft

We are a trusted provider of public cloud, private cloud, hybrid cloud, data center, and disaster recovery solutions with a 20-year history of providing award-winning services.

Our mission is simple yet audacious: **To deliver on the promise of technology.**

As an AWS Managed Service Provider, Public Sector Partner, Government Competency Partner, and DevOps Competency Partner, we focus on AWS public and hybrid cloud environments to design, build, operate, secure, and scale unique technology solutions with a singular purpose: to deftly deliver on the promise of technology for you and your customers.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Configuration Management

Are patching and updates automated?

Manual application of patch and update pro- cesses across operating systems (OS) and software contained within the OS repository is a leading cause of error and system down- time. Make sure patching and updates can be applied with- out human intervention via manual processes.

Do you use a configuration management tool?

A configuration management tool can configure a new server within minutes with less potential for error. It makes sure all configuration pro- cesses are contained in code and applied via automated systems.

Is audit logging configured across the entire cloud platform?

Comprehensive audit logging is not automati- cally acti- vated when you deploy your cloud, and standard cloud logs don't cover all areas. To log all activities across the entire cloud platform, enable comprehensive logging and be sure all log data is sent to CloudWatch and your baseline metrics are established. Next, create CloudWatch Dashboards that present the appropriate system- and busi- ness-level views for your organization.

Do you have formal processes for cloud access?

Pre-defined and clearly communicated pro- cesses and governance rules for cloud access and control credentials will minimize the time needed to manage these requests. Clear pro- cesses also lower the overall risk associated with improperly allocated or configured credentials.

Do you have formal processes defined for management and configuration of all stan- dard software components and repositories that are part of the Operating System (OS) environment?

Often overlooked, standard software components and the repositories that are part of the OS envi- ronment must be accounted for and managed. Consistent processes here will lower the overall risks associated with system updates and ensure patch and update processes are aligned.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Backup and Resilience

Are your volume snapshot/backup configurations and restore processes in line with your governance and compliance policies?

Our standard volume retention policies take daily snapshots at 35 or 90 days. Yet backups alone do not guarantee you can restore or recover data within the required timeframes. Quick discus- sions with your compliance and governance teams can align these processes and mitigate any risks.

Are your long-term data retention processes in line with your governance and compliance policies?

Long-term retention is designed for snapshots, backups, and data where availability require- ments exceed the standard 35 or 90-day system configurations. Note that the time required to execute restore requests of data or files in long- term retention will vary. Again, a discussion with your compliance and governance teams will align these timeframes and help mitigate any risks.

Do you conduct regular testing of file and volume restore processes?

Testing file and volume restore processes is one of the most overlooked responsibilities in IT. Scheduling and conducting quarterly testing can save you hours when a specific restore request arrives at the least expected time.

Do you conduct regular testing of long-term data restore processes?

Long-term data restore processes are another often overlooked responsibility. Scheduling and conducting predefined, quarterly testing – and understanding exactly how long it will take to recover different types of data – can save you hours.

Do you have a formal disaster recovery (DR) plan with testing drills?

There is no standard cloud DR plan. Schedule twice-yearly DR tests to make sure that you can restore critical systems promptly should a disaster occur.

Changes occur often in cloud environments. Make sure your recovery plans reflect those changes.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

User Access Control

Do you have defined cloud account procurement and management processes?

Inconsistent or non-existent processes for account control and management are a lead- ing cause of runaway cloud spending. Defining these processes, and ensuring their adherence, is a critical success factor. Also, if you plan to apply business-unit level billing or chargeback pro- cesses, it must be set up first – here – or you may be rearchitecting your environment to support it.

Do you have defined cloud user (IAM/RBAC) and user access change control processes?

This standardized management process ensures consistency across your cloud platform and full alignment with all governance, security, and compliance requirements. Defining these pro- cesses, and ensuring their adherence, is a critical security requirement.

Are multiple, OS-level User Account Controls (UACs) consistent?

Inconsistencies in OS-level UACs are common, especially with multiple platforms deployed. Whether your environment uses Active Directory, LDAP, SSH, or all three control platforms, you need to define, implement, and manage stan- dardized processes to ensure consistency across your cloud platform and full alignment with all governance, security, and compliance requirements.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

DevOps

Do you use standard processes for Infrastructure as Code (IaC) development and deployment?

The development of IaC automation and IaC automation templates dramatically decreases the opportunity for human error to occur during standard deployment processes. Identifying best practice IaC processes ensures consistency and reliability of your cloud platform and minimizes mistakes that may affect cloud environment or application/data performance.

Have you implemented a Continuous Integration/Continuous Deployment method?

While many CI/CD tools and processes exist, best practices are only effective when customized to your business. If you haven't invested the time to define and deploy your CI/CD model or review adopted CI/CD best practices for their alignment with your environment and business, do so.

Are you annotating your documentation?

Documentation can be unwieldy, annotating it even more so. Take advantage of the cloud's ability to automate the creation of annotated documentation after every build. The outcome of these processes can then be used as an input to your operations code and save your team countless hours of manual work.

Have you adopted application lifecycle management?

Application Lifecycle Management (ALM) is the people, tools, and processes that manage an application from birth to death. ALM leads to continuous delivery of software and updates with releases as often as several times per day vs. every few months.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Monitoring & Alerting

Do you use agent-based OS health and perfor- mance monitoring tools?

While many health and performance monitoring tools exist, we recommend using agent-based systems to provide performance and health sta- tistics from the OS itself. In addition to system availability information, use including CPU, band- width, memory, disk, and other critical variables are also monitored via agent-based systems. The increased monitoring depth adds more data to the equation, but you'll be thankful you have it readily available when you need it.

Have you deployed endpoint health and per- formance monitoring tools?

Easy to deploy and manage but often overlooked, endpoint health and performance monitoring tools are more important now than ever before. During setup and deploy- ment, make sure the comprehensive logging values are selected so you have all available data readily available when you need it.

Have you implemented advanced network performance monitoring tools?

Properly configured network performance mon- itoring tools will detect issues before they are noticed by end users and can reduce mean time to resolution (MTTR) by up to 40%.

Are your application health and performance monitoring tools cloud-native?

Utilizing cloud-native application health and performance monitoring is critical, as they auto- matically consider underlying and connected cloud services, whereas non-cloud-native tools do not.

Are your infrastructure alert tools properly configured?

Make sure you are alerting on all aspects of your cloud infrastructure you care about – not just the default config- uration. The alerts should also include the detail necessary for the alert to be effectively triaged.

Have you deployed AI/ML correlation for system events, alerts, and log analysis?

Proper configuration and management of AI/ML correla- tion services will have a material impact on your business. These services focus primarily on non-threshold-based alerting and minimiz- ing false positives (not actionable incidents) to reduce cost and improve system operational effi- ciency and effectiveness. AI/ML correlation can reduce false positive alerts over 60% when prop- erly configured.

Have you implemented cloud environment change management monitoring?

Change in cloud environments is frequent and normal. However, changes outside of formal change management process need immediate attention to mitigate serious secu- rity, governance, compliance, and cost risk factors.

Have you implemented environment usage delta processes?

Environment usage focuses on the entire cloud environ- ment, including applications, infrastruc- ture, and cloud-na- tive services. Oversight for all usage variance within the cloud's normal daily operating environment is critical as unexpected changes in utilization (bandwidth, compute, memory, storage, cloud-native services, etc.) may show an anomaly that requires immediate response to address security issues or remain within cost thresholds.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Optimize Your AWS Environment

With unparalleled experience and unmatched humanity, we can investigate your AWS environments to make recommendations that optimize your cloud performance while minimizing your cloud spend.

Reach out today for a cloud assessment with our certified Cloud Consulting Team.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Additional Questions

For more information, visit www.deft.com or contact us at (312) 829-1111 and sales@deft.com

About Deft

At Deft, we are our clients' most Trusted Advisor.

The Deft team humanizes technology. We actively listen to our clients, learning and collaborating to develop tailored proposals that perfectly fit your company's needs.

We then design, build, operate, secure, and scale unique technology solutions with a singular purpose: to deftly deliver on the promise of technology for you and your customers.

Learn more at www.deft.com or contact us at (312) 829-1111.