Microsoft

Monitoring Linux Workloads on Azure Learning Series

Module 4

Anthony de Lagarde
September 19, 2024

Reminders & Resources

All Workshops are recorded, and you can access all Recordings for your viewing replay.

Survey & Feedback. Please provide your inputs on the Learning content and format on the survey.

You can always send general feedback and commit GitHub Push Requests to merge contents

Join the Microsoft Open-Source community

Your presenters

Anthony de Lagarde
Principal Engineer
Azure CXP FastTrack for Azure

- 17 years with Microsoft
- Working with Azure since 2015
- Career supporting Financial Services, Healthcare, US Federal Government, and State and Local Government
- Working with Open-Source since 1998 (FreeBSD, Linux, and various projects supporting various business solutions)

Goals

This session aims to help the Microsoft's technical community review recommended practices monitoring Linux workloads in Azure. This session is geared towards using Azure native monitor tooling

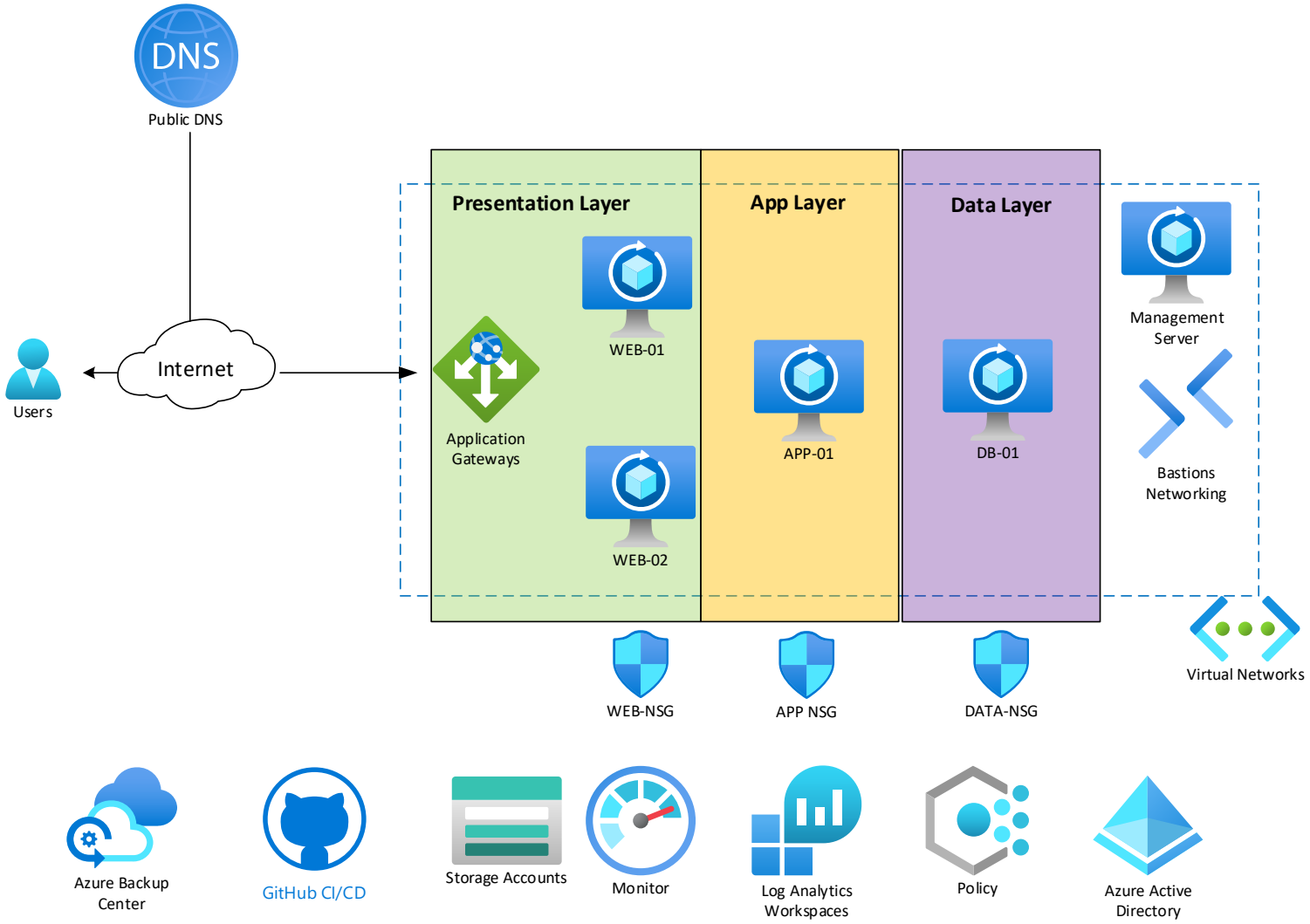
Agenda

- Three-Tier application overview
- Monitoring Consideration
- Monitoring Recommendations
- Q & A
- LAB

Planning

Design Considerations and Recommendations

Three-Tier Application Overview



Monitoring Considerations

Consult with the customer or partner on their current monitoring solution and intent.

Engage with the application owners, architects, and developers to get a firm understanding of the application profile as well as system design limits

Are there any external dependencies that are critical for the application to operate as intended

Identify the application personas. Will access come from internal or external networks and how will users authenticate against the application

Review the customer administration model. Understand the required RBAC roles to implement Azure Monitor. Please review the following guidance Roles, permissions, and security in Azure Monitor - Azure Monitor | Microsoft Learn

Understand the customers industry vertical to validate if there are specific regulatory requirements and monitoring retention

Validate name resolution within the application and hybrid requirements

Has redundancy been implemented in the design and are there any SLA's?

Will the monitoring solution be required to initiate an application failover?

Please refer to the following Designing multi-tier web application built for HA/DR - Azure Architecture Center

You can also refer to Azure Monitor Baseline Alerts for additional guidance and counters based on on Azure components selected in the design of the application

Syslog/rsyslog/syslog-ng
Will the customer or partner plan on leveraging syslog/syslog-ng for capturing both security and system metrics. Recommend integrating Syslog with Log Analytics to avoid bifurcation of data. Please note as of August 2024 the Log analytics agent for Linux will be deprecated with no further support. You need to migrate your clients to Azure monitor. Please read the following article Azure monitor agent migration

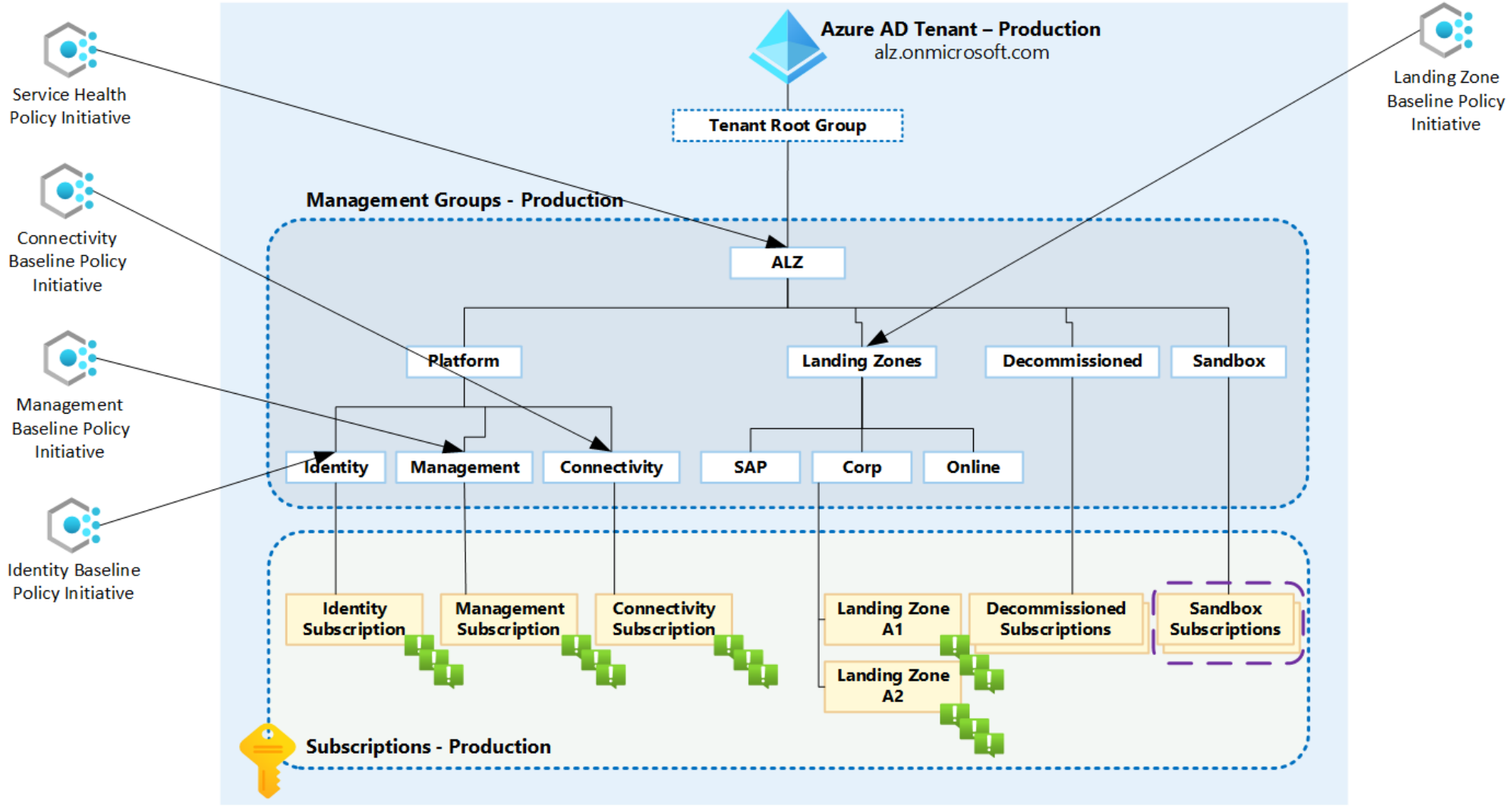
Please review Collect Syslog data sources with the Log Analytics agent in Azure Monitor - Azure Monitor | Microsoft Learn

Monitoring Recommendations

- **Implementation:** Implement an initial set of metrics and limit potential "*white noise*" and gradually add required counters
- Conduct an initial validation of the monitoring solution and how will it integrate with their current organizational structure
- Establish monitoring prior to the customers data migration phase and before going into production
- **Visualization:** Build custom dashboards in the Azure portal to visualize key metrics and logs. This provides a centralized view of the application's health and performance
- **Notifications:** Implement email notifications, SMS alerts, Logic Apps, Azure automation runbooks, and ITSM tooling to enable additional capabilities integrating with the customers ticketing system as part of overall monitoring strategy
- **Web Tier:** Integrate Application Insights with your web tier to monitor the performance, availability, and usage of your web applications. This will help you track user interactions and detect anomalies
- **Business Tier:** Use Application Insights to monitor the business logic layer. This includes tracking custom events, exceptions, and performance metrics
- **Data Tier:** Monitor your database performance and query execution times using Azure Monitor
- **Distributed Tracing:** Use Application Insights to implement distributed tracing. This helps you track requests as they flow through different components of the application, making it easier to diagnose performance issues and failures
- **Continuous Improvement:** Regularly review the collected data and adjust monitoring strategy as needed. Use the insights gained to optimize the application's performance and reliability
- **Recommendations Syslog/Syslog-ng/rsyslog**: Encourage the customer or partner to integrate their native logging solution with Log Analytics. Ensure local applications like NGINX or Apache write to Syslog rather than to their native logs. **Do not enable every** alert possible whit syslog. Concentrate on the following:

Authentication errors
Authpriv warnings
Errors
Kernel warning

Monitoring Recommendations Azure Policy & AMBA



Monitoring Linux Workloads in Azure Lab

Module 4: Monitoring Linux Workload Lab

Q & A

Links & Resources

Azure Monitor Baseline Alerts Introduction video

Azure Monitor Baseline Alerts Home Page

Introduction to deploying AMBA ALZ Pattern

AMBA GitHub Repo

CentOS End-of-Life guidance

Linux and Open Source on Azure Quarterly Update -July 2024

Collect Syslog events with Azure Monitor Agent - Azure Monitor | Microsoft Learn

Module 4: Monitoring Linux Workloads in Azure Lab

Thank you