Top 10 Azure Security Best Practices

Gregor Reimling
About “Gregor Reimling”

- **Focus**: Azure Governance, Security and IaaS
- **From**: Cologne, Germany
- **My Blog**: https://www.Reimling.eu
- **Certifications**: Cloud Architect & MVP for MS Azure
- **Hobbies**: Family, Community, Worldtraveler
- **Contact**: @GregorReimling, @CloudInspires

Azure Meetup
BONN
azurebonn

www.azurebonn.de
www.cloudinspires.me
Important Dates

Effective October 1, 2022, we will begin to permanently disable Basic Authentication for Exchange Online in all Microsoft 365 tenants regardless of usage, except for SMTP Authentication. Read more here.

Retiring Azure AD Connect 1.x versions

Important

On August 31, 2022, all 1.x versions of Azure AD Connect will be retired because they include SQL Server 2012 components that will no longer be supported. Upgrade to the most recent version of Azure AD Connect (2.x version) by that date or evaluate and switch to Azure AD cloud sync.
1. Enterprise Scale
**MS Cloud Adoption Framework**

**Define Strategy**
- Understand motivations
- Business outcomes
- Business justification
- Prioritize project

**Plan**
- Digital estate
- Initial organization alignment
- Skills readiness plan
- Cloud adoption plan

**Ready**
- Azure readiness guide
- First landing zone
- Expand the blueprint
- Best practice validation

**Adopt**
- Migrate
  - First workload migration
  - Expanded scenarios
  - Best practice validation
  - Process improvements
- Innovate
  - Innovation guide
  - Expanded scenarios
  - Best practice validation
  - Process improvements

**Govern**
- Methodology
- Benchmark
- Initial best practice
- Governance maturity

**Manage**
- Business commitments
- Operations baseline
- Ops maturity

---

Enterprise-Scale - Design Principles

- Tenant Root Group
- Build Clouds

**Autonomy for Innovation**
(Subscription Democratization)

**Security and Compliance “By-Default”**
(Azure Native Design/Platform Alignment)

**Policy-Driven Governance**
(Single Control/Management Plane)
GitHub Enterprise Scale Templates

Deploy Enterprise-Scale with Azure VWAN

GitHub - Azure/Enterprise-Scale: The Azure Landing Zones (Enterprise-Scale) architecture provides prescriptive guidance coupled with Azure best practices, and it follows design principles across the critical design areas for organizations to define their Azure architecture.
Azure Tenant Design approach

- Tenant Root Group
- Build Clouds
- BC- Platform
- BC- Connectivity
- Sub Connectivity
- Sub vWAN
- BC- Identity
- Sub Identity
- BC- Landing Zones
- Sub Infrastructure
- Sub AVD
Well-architected Framework

Cost Management

Security

Reliability

Performance Efficiency

Operational Excellence

Azure Well-Architected Framework

“The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload.”

https://docs.microsoft.com/en-us/azure/architecture/framework/
Demo

Dive into the Azure Portal
• Enterprise Scale
• Azure Advisor
2. Hybrid Identity
Enable PHS and forgot ADFS
# Azure AD Cloud Connect Sync

<table>
<thead>
<tr>
<th>Feature</th>
<th>Connect Sync</th>
<th>Cloud Sync</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to multiple disconnected on-premises AD forests</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Lightweight agent installation model</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiple active agents for high availability</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect to LDAP directories</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Support for device objects</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Support for device writeback</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Support for group writeback</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Support for Pass-Through Authentication</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Temporary Access Pass

https://aka.ms/mysecurityinfo
Azure AD Recommendations

- Block Legacy Auth
- Go Passwordless
- Regularly Update AAD Connect
- Use Conditional Access
- Use TAP for new Employees
- Use Hybrid Devices
- Use Secure Score for Identity
- Use CAE
- Evaluate AAD Cloud Connect Sync
- Enable PIM
- Enable PIM
- Use TAP for new Employees
3. Identity Secure Score
Identity Protection with Conditional Access

• Enable CAE (Conditional Access Evaluation)
  • To minimize lag in Token lifetime
  • User termination or password change/reset revocation will be enforced in near real time
Show following settings
• Identity Secure Score
4. PAW
Privileged Access Devices

Why are privileged access devices important | Microsoft Learn
Privileged Admin Workstation

- Use dedicated VMs for managing Azure/Microsoft 365 environments
- Use this VMs only for administration tasks
- Do not enable Internet- / Social media access on this VMs
- Enforce Device compliance via Conditional Access for this VMs
- Use AVD as PAW solution
5. Network
# Azure IaaS Recommendations

- **Segmentation of Virtual Networks**
- **Define Subnets and use NSG at Subnet Level**
- **Use a NVA or Azure Firewall at the Hub Network**
- **Define UDR to Route traffic over the Hub Network and Firewall**
- **Use Azure Web Application Firewall for Internet applications**
- **Use DDoS Protection for Web Applications**
- **Use Azure Bastion for VM Management**
## Azure Firewall Editions

### New in Public Preview (MS Ignite 2022)

<table>
<thead>
<tr>
<th>Azure Firewall Basic</th>
<th>Azure Firewall Standard</th>
<th>Azure Firewall Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 VMs fixed under the hood</td>
<td>Built-in high availability</td>
<td><strong>All from Standard</strong> +</td>
</tr>
<tr>
<td>Availability Zones</td>
<td>Availability Zones</td>
<td>TLS Inspection</td>
</tr>
<tr>
<td>App FQDN Filtering Rules?</td>
<td>Application FQDN Filtering Rules</td>
<td>IDPS</td>
</tr>
<tr>
<td>Fixed Scale</td>
<td>Unrestricted Cloud Scalability</td>
<td>URL Filtering</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Threat Intelligence</td>
<td>Web categories</td>
</tr>
<tr>
<td>(Alert Mode only)</td>
<td>FQDN in Network rules</td>
<td>FQDN in Network rules</td>
</tr>
<tr>
<td>FQDN in Network rules</td>
<td></td>
<td>30GBps</td>
</tr>
<tr>
<td>250-500MBps</td>
<td></td>
<td>Around XXX€</td>
</tr>
<tr>
<td>Around XXX€</td>
<td></td>
<td>901,24€ per month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1,262,29€ per month</td>
</tr>
</tbody>
</table>

- **Azure Firewall Basic**: 2 VMs fixed under the hood, Availability Zones, App FQDN Filtering Rules?, Fixed Scale, Threat Intelligence (Alert Mode only), FQDN in Network rules, 250-500MBps, Around XXX€.
- **Azure Firewall Standard**: Built-in high availability, Availability Zones, Application FQDN Filtering Rules, Unrestricted Cloud Scalability, Threat Intelligence, FQDN in Network rules, 30GBps, 901,24€ per month.
- **Azure Firewall Premium**: All from Standard, TLS Inspection, IDPS, URL Filtering, Web categories, FQDN in Network rules, 30GBps, 1,262,29€ per month.

(Actual pricing and services may vary.)
AZURE

6. MS Defender for Cloud
Microsoft Defender for Cloud

- **Continuously Assess**
  Know your security posture.
  Identify and track vulnerabilities.

- **Secure**

- **Defend**
  Detect and resolve threats to resources and services.

Asset icons:
- Cosmos DB
- Container
- Web App
- Azure DNS
- Virtual Machines
- Key Vault
- Ressources
- Storage Accounts
- SQL Services
Security posture & compliance

Secure score

Asset management

Policy

Server protection (Microsoft Defender for Cloud for VMs)

Threat detection

VA (power by Qualys)

Application control

Automation & management at scale

Automation

SIEM integration

Export
## Defender for Servers Plans

<table>
<thead>
<tr>
<th>Feature</th>
<th>Plan 1</th>
<th>Plan 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified View</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic MDE provisioning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MS Threat and Vulnerability management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Policy and Regulatory Compliance</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated Vulnerability by Qualys</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Log Analytics 500MB free data ingestion per day</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Threat detection</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Adaptive application control</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>File integrity monitoring</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Just-in-Time VM access</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Adaptive Network hardening</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Docker host hardening</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Fileless attack detection</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Price</strong></td>
<td>$5 per Server</td>
<td>$15 per Server</td>
</tr>
</tbody>
</table>

Demo

Dive into the Azure Portal
• Microsoft Defender for Cloud
7. Microsoft Sentinel
8. Azure Arc
Azure Arc
Azure Arc: at a high level

Bring Azure services and management to any infrastructure, anywhere

Run Azure data services anywhere
Extend Azure management across your environments
Adopt cloud practices on-premises
Implement Azure security anywhere

Azure Arc is a set of technologies that extends Azure management and enables Azure services to run across on-premises, multi-cloud, and edge
Update Management Center (preview)

- New solution for centrally Update Management across different environments
- No dependencies to Log Analytics Agent
- Fully support for Azure Arc managed VMs
- Support Windows and Linux VMs
- Support automatic VM guest patching
- Support Hot patching
- Is in preview wait for production until release going to GA
Defender CSPM plan was enabled recently on at least one of your subscriptions/accounts. It could take up to one day until all data will be available.
Defender for DevOps

Join Our Security Community - Microsoft Community Hub
Training | Microsoft Learn

Join Our Security Community - Microsoft Tech Community
Zero Trust architecture
Microsoft Cybersecurity Reference Architectures (MCRA)

**Capabilities**
What cybersecurity capabilities does Microsoft have?

**People**
How are roles & responsibilities evolving with cloud and zero trust?

**Zero Trust User Access**
How to validate trust of user/devices for all resources?

**Azure Native Controls**
What native security is available?

**Security Operations**
How to enable rapid incident response?

**Multi-Cloud & Cross-Platform**
What clouds & platforms does Microsoft protect?

**Secure Access Service Edge (SASE)**
What is it? How does it compare to Zero Trust?

**Attack Chain Coverage**
How does this map to insider and external attacks?

**Operational Technology**
How to enable Zero Trust Security for OT?
Top 5 Must have Settings

1. Enable Multifactor Authentication
2. Enable and Integrate Conditional Access
3. Use Azure Advisor recommendations
4. Cloud Security Posture Management is needed
Conclusion

1. Enterprise Scale
2. Identity Secure Score
3. Use WHfB and TAP
4. Azure AD Cloud Sync
5. PAW
6. Network
7. Defender for Cloud
8. Microsoft Sentinel
9. Side Notes
10. Learning
• Reimling.eu – Microsoft will disable Basic auth – What this means and what you have to do
• Block legacy authentication - Azure Active Directory - Microsoft Entra | Microsoft Docs
• Deprecation of Basic authentication in Exchange Online | Microsoft Docs
• Common Conditional Access policies - Azure Active Directory - Microsoft Entra | Microsoft Learn
• Configure a TAP in Azure AD to register Passwordless authentication - Microsoft Entra | Microsoft Docs
• Azure AD Connect: Version release history - Microsoft Entra | Microsoft Docs
• Zero Trust security in Azure | Microsoft Docs
• Enterprise-Scale/README.md at main · Azure/Enterprise-Scale · GitHub
• Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs
• Azure Arc | Microsoft Learn
• Update management center (preview) overview | Microsoft Docs
• Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
• Join Our Security Community - Microsoft Tech Community
• Managed identities for Azure resources - Microsoft Entra | Microsoft Learn
• Microsoft Certified: Azure Security Engineer Associate - Certifications | Microsoft Learn
About “Gregor Reimling”

Blog
• https://www.Reimling.eu

Contact
• @GregorReimling
• @CloudInspires

Thank You