Back from MS Build 2021 - Security Session

Maxime Coquerel - MVP Azure

Speaker

Maxime Coquerel

Director Cloud Security Architect

Email : max.coquerel@live.fr

Blog : zigmax.net (since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

Open Source Contributor (Kubernetes / VSCode)

Disclaimer

“*Any views or opinions expressed in this presentation are those of the presenter and not necessarily represent the view and opinions of my employer, its ownership, management or its employees .*“

Thank you!

Communauté Microsoft Azure Québec

Québec, QC
1090 membres · Groupe public
Organisé par **Tidjani B.** et **3 autres personnes**

Partager :

Réseau **.NET Foundation – 385 groupes**

DotNet Québec

Québec, QC
425 membres · Groupe public
Organisé par **Hinault D.**

Partager :

Session Agenda / Goal

- **Azure Kubernetes Service**
  - AKS | Azure RBAC for Kubernetes Authorization
  - AKS | FIPS (Preview)
  - AKS Host Support Encryption

- **Azure Cosmos DB**
  - Azure Cosmos DB | Always Encrypted
  - Azure Cosmos DB | RBAC

- **Azure Confidential**
  - Azure Confidential | Ledger
  - Azure Confidential | Azure SQL Database ledger

AKS

AKS | Azure RBAC for Kubernetes Authorization

With Azure role-based access control (RBAC) for Kubernetes authorization, you can achieve unified management and access control across Azure and AKS resources.

With this capability, you can now manage RBAC for AKS and its resources using Azure or native Kubernetes mechanisms. When enabled, **this integration allows you to use Azure Active Directory (AAD) users, groups, or service principals as subjects in Kubernetes RBAC**. This frees you from having to separately manage user identities and credentials for Kubernetes.

https://azure.microsoft.com/en-us/updates/general-availability-azure-rbac-for-kubernetes-authorization-in-aks/

AKS | FIPS (Preview)

The Federal Information Processing Standard **(FIPS) 140-2 is a US government standard** that defines minimum security requirements for cryptographic modules in information technology products and systems. AKS allows you to create Linux-based node pools with FIPS 140-2 enabled. Deployments running on FIPS-enabled node pools can use those **cryptographic modules** to provide increased security and help meet security controls as part of FedRAMP compliance.

https://azure.microsoft.com/en-us/updates/preview-aks-support-for-fips-compliant-nodes/

https://zigmax.net/aks-fips/

AKS Host Support Encryption

With host-based encryption, the **data stored on the AKS agent nodes is encrypted at rest**. This capability provides an additional measure of security as the data is encrypted end-to-end.

This means the temp disks are encrypted at rest with platform-managed keys. The cache of OS and data disks is encrypted at rest with either platform-managed keys or customer-managed keys depending on the encryption type set on those disks.

https://docs.microsoft.com/en-us/azure/aks/enable-host-encryption

https://azure.microsoft.com/en-us/updates/general-availability-encryption-at-host-support-in-aks/

Cosmos DB

Azure Cosmos DB | Always Encrypted

Always Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure Cosmos DB. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the database.

Always Encrypted brings client-side encryption capabilities to Azure Cosmos DB. Encrypting your data client-side can be required in the following scenarios:

- Protecting sensitive data that has specific confidentiality characteristics: **Always Encrypted allows clients to encrypt sensitive data inside their applications and never reveal the plain text data or encryption keys to the Azure Cosmos DB service.**
- Implementing per-property access control: Because the encryption is controlled with keys that you own and manage from Azure Key Vault, you can apply access policies to control which sensitive properties each client has access to.

https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-always-encrypted?tabs=dotnet
https://azure.microsoft.com/en-us/updates/always-encrypted-for-azure-cosmos-db-in-public-preview/

Azure Cosmos DB | RBAC

With Azure Cosmos DB role-based access control now available for Core (SQL) API, you can enable fine-grained access control by assembling allowed actions into role definitions and assigning these roles to Azure Active Directory (AAD) identities.

The Azure Cosmos DB data plane RBAC is built on concepts that are commonly found in other RBAC systems like **Azure RBAC**:

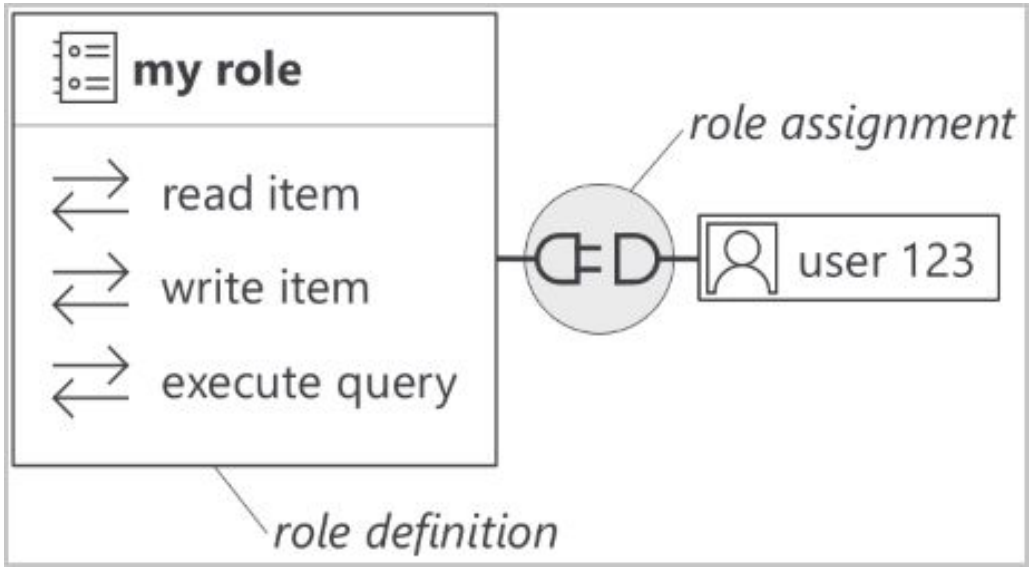
- The **permission model** is composed of a set of actions; each of these actions maps to one or multiple database operations. Some examples of actions include reading an item, writing an item, or executing a query.
- Azure Cosmos DB users create **role definitions** containing a list of allowed actions.
- Role definitions get assigned to specific Azure AD identities through role assignments. A role assignment also defines the scope that the role definition applies to; currently, three scopes are currently:
    - An Azure Cosmos DB account,
    - An Azure Cosmos DB database,
    - An Azure Cosmos DB container.

https://azure.microsoft.com/en-us/updates/azure-cosmos-db-rolebased-access-control-rbac-now-in-general-availability/

Azure Cosmos DB | RBAC

Role definitions get assigned to specific **Azure AD identities through role assignments**. A role assignment also defines the scope that the role definition applies to; currently, three scopes are currently:

- An Azure Cosmos DB account,
- An Azure Cosmos DB database,
- An Azure Cosmos DB container.



https://azure.microsoft.com/en-us/updates/azure-cosmos-db-rolebased-access-control-rbac-now-in-general-availability/

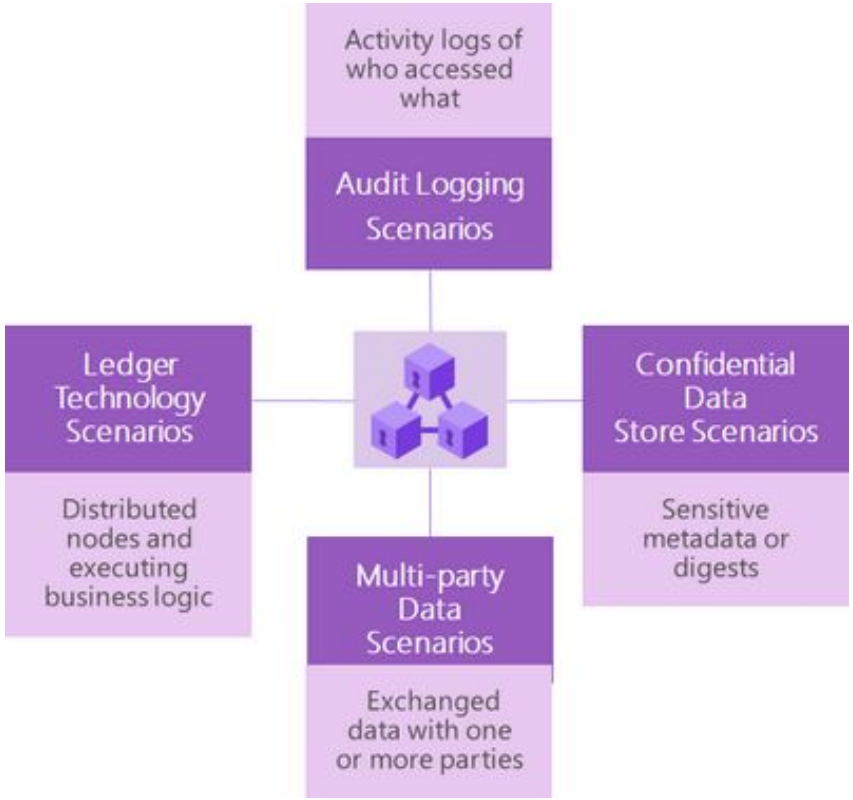
Azure Confidential

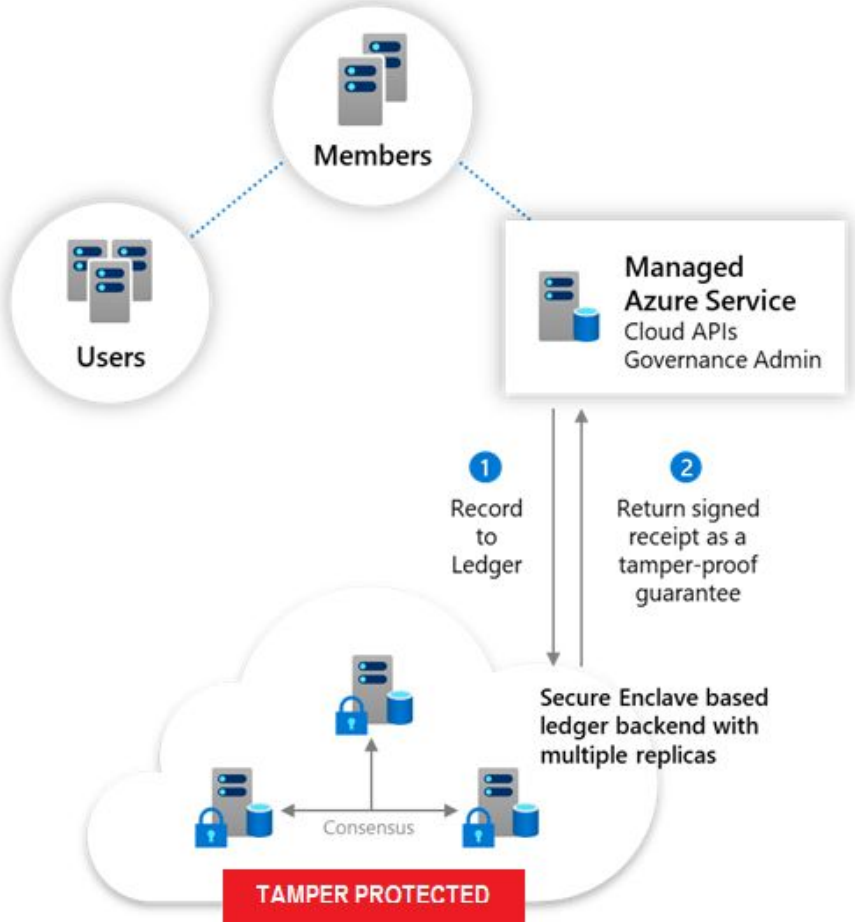
Azure Confidential | Ledger

Azure Confidential Ledger (ACL), a fully managed service that provides the ability to **store sensitive data records with integrity and confidentiality protections**, all in a highly available and scalable service. Using ACL, customers can store data in an immutable, tamper-protected, and append-only ledger. The service provides these assurances by harnessing the power of Confidential Computing's hardware-encrypted secure enclaves when setting up the decentralized blockchain network, limiting Microsoft's access to operating the nodes in the ledger.

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/record-confidential-transaction-logs-with-azure-confidential/ba-p/2377226

Azure Confidential | Ledger





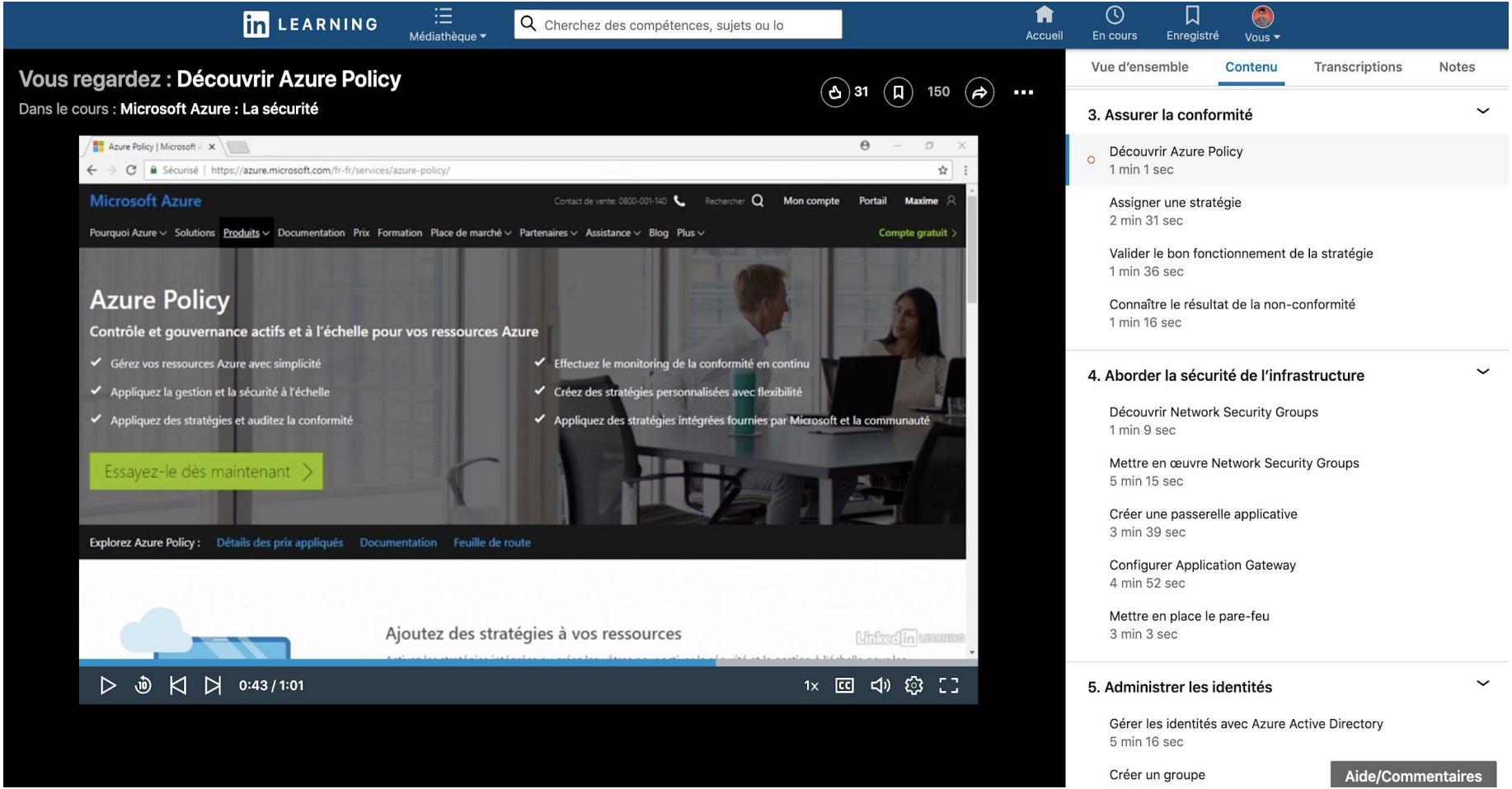
Azure Confidential | Azure SQL Database ledger

Azure SQL Database ledger, which adds tamper-evident capabilities to your Azure SQL Databases, available in Preview starting in West Central US with all regions following shortly.

With the ledger feature, **you will be able to detect if data in your Azure SQL Database has been maliciously altered and if so, restore it back to the original value.** Using the same cryptographic patterns seen in blockchain technology, each transaction is cryptographically hashed and inserted in a blockchain data structure. The computed hashes of your database are then stored outside of Azure SQL Database in tamper-proof storage (such as Azure immutable Blob storage, or Azure Confidential Ledger), as database digests. Database digests are used later to verify that data in the database has not been tampered with, by comparing the hash values in the digests against the calculated hashes stored in Azure SQL Database ledger. If even a single bit is altered in the database, the database verification process will detect and report the tampering.

Azure SQL Database ledger provides two types of ledger-enabled tables for your database: **updatable ledger tables** and **append-only ledger tables**.

https://azure.microsoft.com/en-us/updates/azure-sql-database-ledger-available-in-public-preview/



Source: https://www.linkedin.com/learning/microsoft-azure-la-securite/decouvrir-azure-policy

Technical Resources

Microsoft Build 2021 - https://mybuild.microsoft.com/

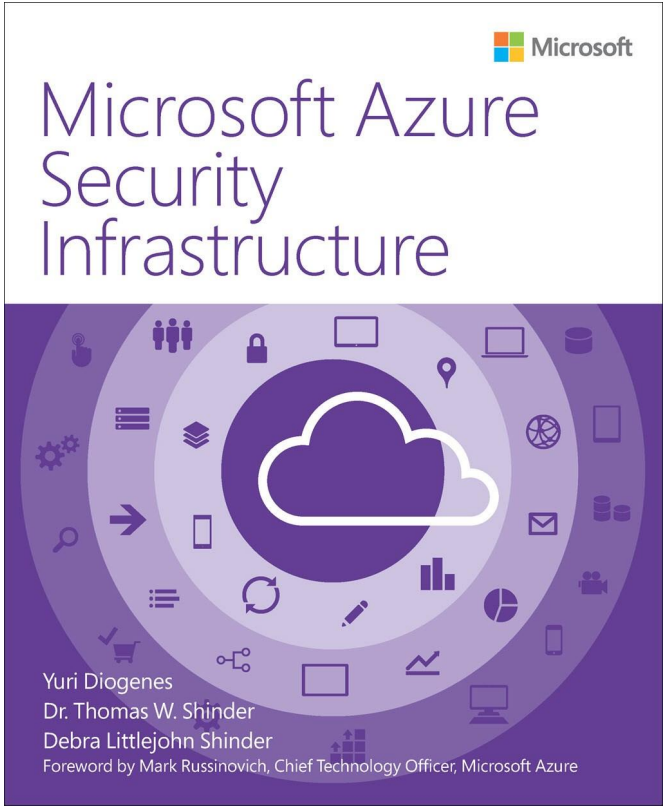
Microsoft Technical Community Content
https://github.com/Microsoft/TechnicalCommunityContent

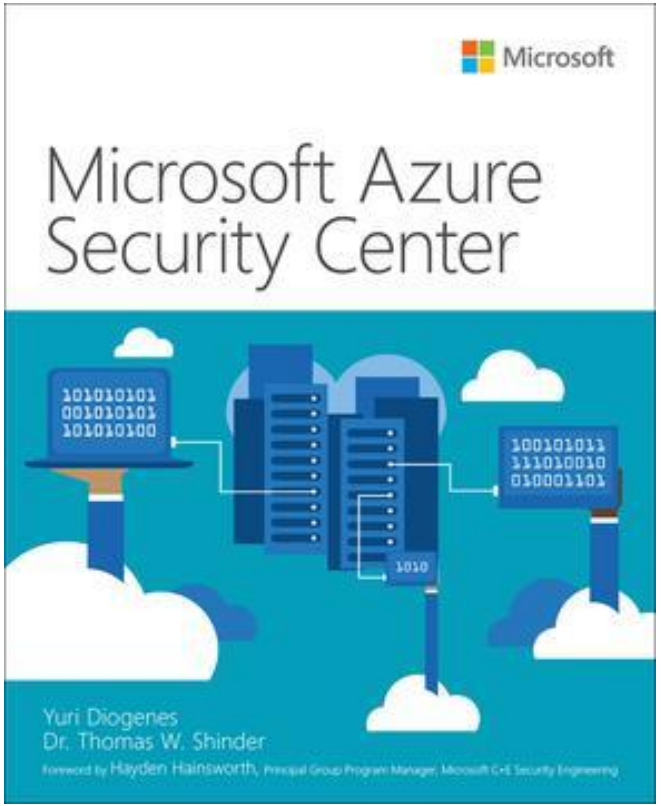
Azure Security Blog - https://azure.microsoft.com/en-us/blog/topics/security/

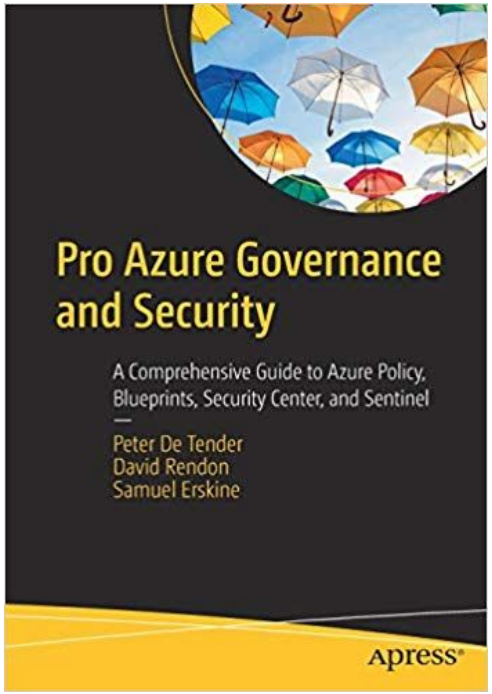
Maxime Blog - http://zigmax.net

Channel Youtube - Communauté Azure Quebec
https://www.youtube.com/channel/UCYLAJgoYFLYf0d4jWXuC1cA

Books


Microsoft
Microsoft Azure Security Infrastructure
Yuri Diogenes
Dr. Thomas W. Shinder
Debra Littlejohn Shinder
Foreword by Mark Russinovich, Chief Technology Officer, Microsoft Azure


Microsoft
Microsoft Azure Security Center
Yuri Diogenes
Dr. Thomas W. Shinder
Foreword by Hayden Hainsworth


Pro Azure Governance and Security
A Comprehensive Guide to Azure Policy, Blueprints, Security Center, and Sentinel
Peter De Tender
David Rendon
Samuel Erskine
Apress

Questions / Talks