



○ Available region
⊙ Announced region
• Availability Zone(s) present

Hvernig er hægt að auka skilvirkni og yfirsýn í rekstri

Microsoft Azure

Efni fyrirlesturs

- *Unstructured Azure umhverfi*
- *Rekstarleg áskorun*
- *Ávinningur á breytingum?*
- *Hvernig förum við að?*
- *Hvaða tæki og tól geta aðstoðað okkur?*
- *Hver væru okkar næstu skref?*

“Unstructured” Azure umhverfi Hvernig endaði ég þar?

Upphafleg stefna

Engin upphafleg stefna eða rammi til þess að halda utan um hraða uppbyggingu á Azure þjónustum

Færsla á þjónustum

Flutningur á þjónustum frá “private cloud” yfir í Azure hefur oftast verið flutt eins og þær voru

Dreifð ávörðunataka og stjórnun

Þegar mörg teymi eða deildir hafa aðgang að Azure auðlindum, þá getur það leitt til ósamræmis á reglum, búið til öryggisholur. Hvernig er yfirsýn rekstaraðila þá?

Ófullnægjandi þjálfun eða sérfræðipekking

Það er mjög mikilvægt að fyrirtæki geri kröfur um að þekkingaröflun á sviði skýjalausna.

Lítil eða engin sjálfvirknivæðing

Villur, vandamál og rekstarörðuleikar má oft koma í veg fyrir með sjálfvirknivæðingu.

Samruni eða yfirtökur

Þegar tveir heimur koma saman í IT, þá er erfitt að ákveða hvaða vegferð á að fara. Oftast á samruni/yfirtaka að gerast mjög fljót og ekki er pláss fyrir skipulagningu

Tölur sem tala (frá Microsoft)

<u>25%</u>	<u>67%</u>	<u>50%</u>	<u>Top 3</u>
<i>Fyrirtæki sem hafa farið í gegnum stefnumótun og hagræðingu hafa að meðaltali sparað 25% af Azure reikningum</i>	<i>67% þeirra fyrirtækja sem tilkynntu öryggistilvik árið 2021 staðfestu að ástæðan hafði verið vegna “misconfiguration”</i>	<i>Þeir sem hafa innleitt sjálfvirknivæðingu, reglur og stefnu segjast hafa stýtt uppsetningartíma á þjónustum um allt að 50%</i>	<i>Þekking á skýjaþjónustum eru meðal þriggja eftstu þátta sem vantar inn hjá fyrirtækjum.</i>

Ávinningur og aðferðir á vel skipulagðri/endurskipulagðri Azure vegferð

“Assessment” á núverandi umhverfi

Allt umhverfið er meðtið, skilningur á hverri einustu þjónustu og tilgangur þeirra skráður

Búum til vegferð til framtíðar (3 – 5 ára)

Þegar allir eru að róa í sömu átt, þá verður skilningur, utanumhald og rekstur mun betri.

Tileinkum okkur sjálfvirknivæðingu

Með sjálfvirknivæðingu í uppsetningu og rekstri er hægt að koma í veg fyrir “misconfiguration” á umhverfi og þjónustum

Aukin skilningur á umhverfi og þjónustum

Með auknum skilningi á umhverfi og þjónustum er hægt að sjá fyrir um kostnað og gert áætlun.

Einfaldari rekstur

Þegar þú hefur alla yfirsýn yfir umhverfið og hefur tileinkað þér sjálfvirknivæðingu eins og með Blueprints eða Terraform, þá verður rekstur og uppsetning mun auðveldari

Skýr ábyrgð og ábyrgðarsvið

Þegar skýr ábyrgð er til staðar og reglur sem styðja við það, þá er hægt að koma í veg fyrir mikið af öryggisholum sem myndast í umhverfinu.

Azure “assessment”

Tæki, tól og aðferðir

- *Microsoft Assessments*
- *ScoutSuite*
- *StormSpotter*
- *Surveil*

Microsoft Assessments

- Azure Well-Architected Review
- Azure Security and Compliance Assessments
- Azure Cost Management Assessment
- Governance Benchmark
- Strategic Migration Assessment and Readiness Tool
- Cloud Journey Tracker

Azure Well-Architected Review

Examine your workload through the lenses of reliability, cost management, operational excellence, security and performance efficiency.

Improve your results

Our recommendations for improving your results are organized by category below.

Recommendations Unanswered Sort By: All

Reliability CRITICAL

39 recommended actions Show more

Security CRITICAL

121 recommended actions Show less

Results breakdown

CRITICAL 0-33 MODERATE 33-67 EXCELLENT 67-100

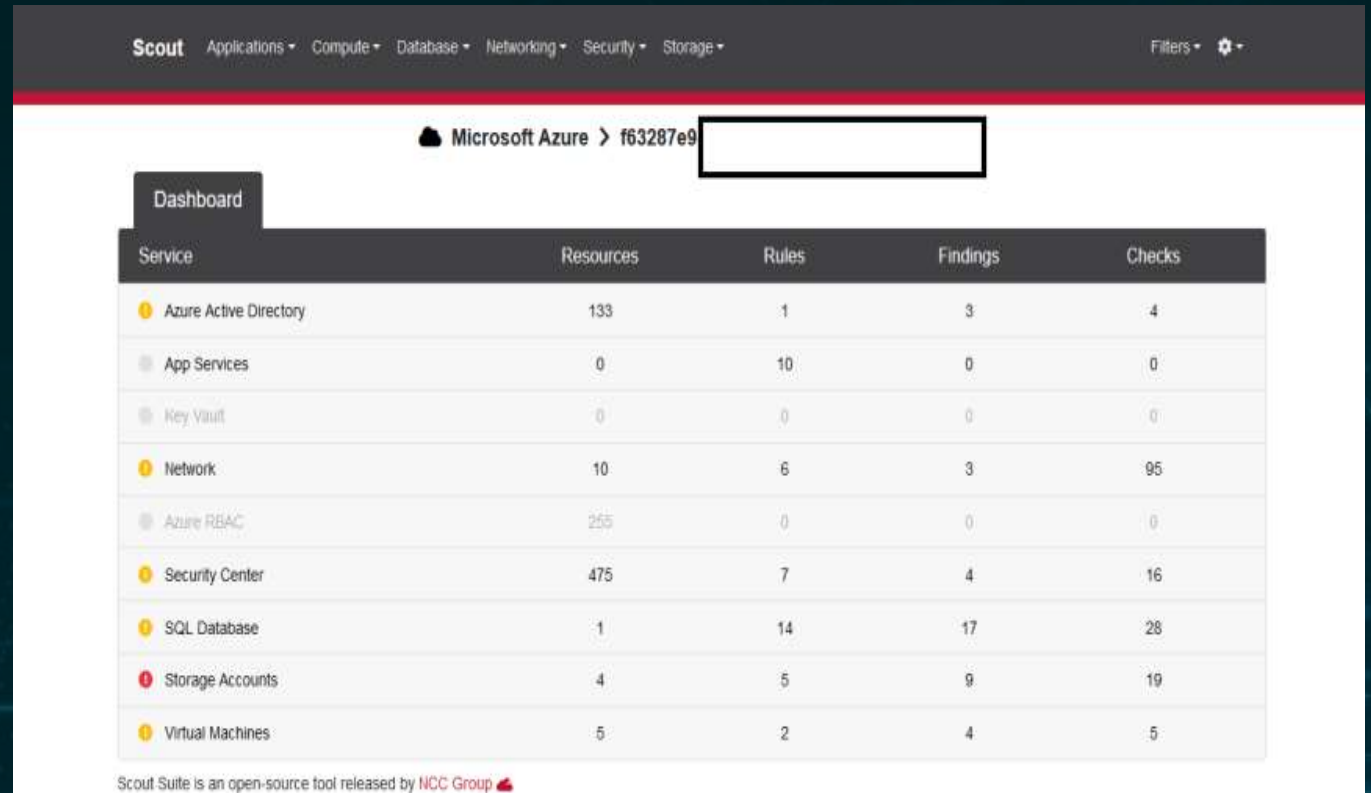
Your result: 0/100

121 recommended actions

<input type="checkbox"/>	Recommendations	Priority	Notes
<input type="checkbox"/>	Configure emergency access accounts	100	Add a Note
<input type="checkbox"/>	Implement threat protection for the workload	100	Add a Note
<input type="checkbox"/>	Adopt threat modeling processes	90	Add a Note
<input type="checkbox"/>	Implement Conditional Access Policies	90	Add a Note
<input type="checkbox"/>	Classify your data at rest and use encryption	90	Add a Note
<input type="checkbox"/>	Protect all public endpoints with appropriate controls	90	Add a Note
<input type="checkbox"/>	Restrict access to backend services to a minimal set of public IP addresses; only those who really need it	90	Add a Note

ScoutSuite

- Open-Source
- Azure/AWS/GCP Security Audit
- Graph API réttindi með Enterprise application
 - Directory.Read.All
 - Policy.Read.All
- Auðvelt í uppsetningu



Scout Suite is an open-source tool released by NCC Group

Service	Resources	Rules	Findings	Checks
Azure Active Directory	133	1	3	4
App Services	0	10	0	0
Key Vault	0	0	0	0
Network	10	6	3	95
Azure REAC	255	0	0	0
Security Center	475	7	4	16
SQL Database	1	14	17	28
Storage Accounts	4	5	9	19
Virtual Machines	5	2	4	5

What is ScoutSuite

Scout Suite is an open-source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments.

StormSpotter

- Open-Source
- Attack Graph
- Keyrt með Service Principal
- Auðvelt í uppsetningu
- Azure Team - Github project

The screenshot displays the StormSpotter interface. On the left, a 'Raw Query' editor contains a Cypher query: `1 MATCH (a:ANDRUIA) RETURN a`. Below the editor is a 'SUBMIT QUERY' button. The central area shows an 'Attack Graph' with nodes representing users and services. Nodes include 'Eden Garza', 'Kathy Yu', 'User Account Administrator', 'Microsoft Azure ServiceFabric', 'Microsoft AzureActiveDirectory', 'Billing Administrator', and 'Directory Reader'. Edges represent relationships like 'MemberOf' and 'HasRole'. On the right, a 'Raw Data' table shows the results of the query.

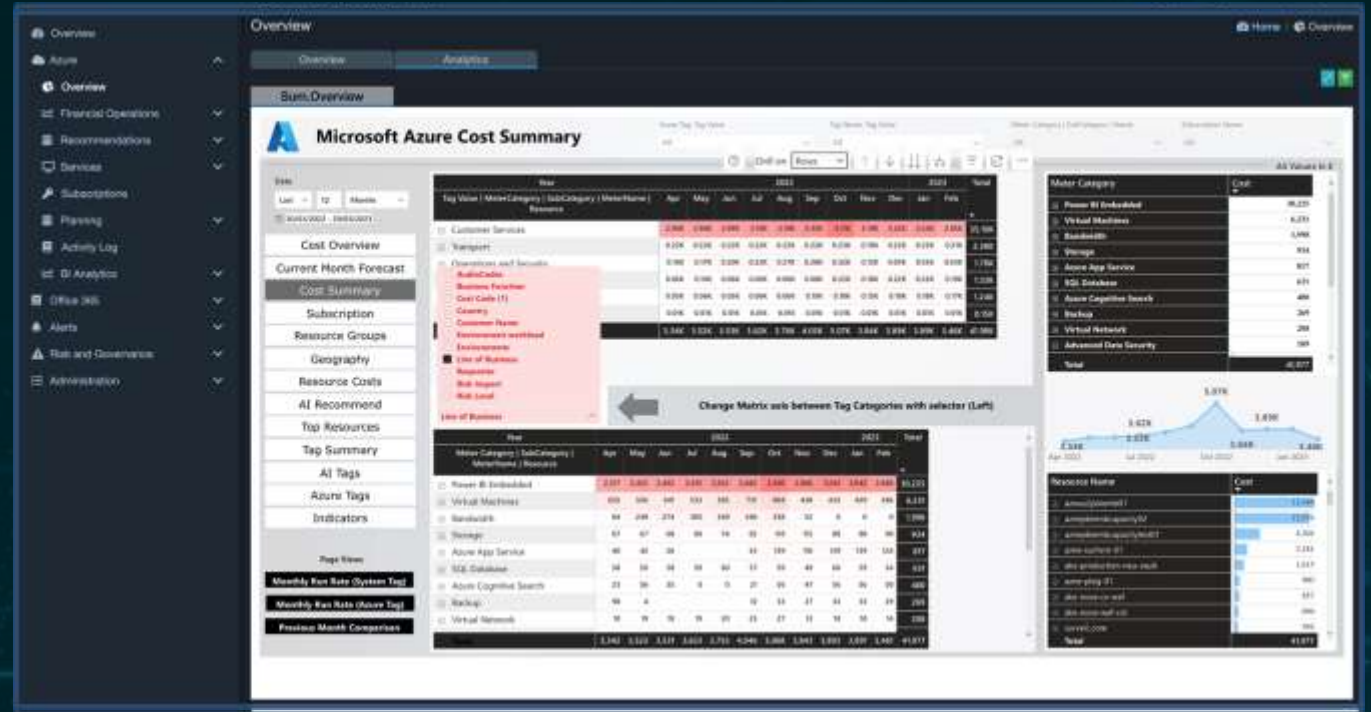
Property #	Value
cloudSecurityIdentifier	5-1-11-1-30284628-120384208-181347781-2976840771
description	Can manage all aspects of users and groups, including resetting passwords for limited users.
id	00000003-0013-4c3f-98df-4bc77f409a31
isSystem	true
members	0bc1716f-8c72-4b49-8d6c-1d780816464c-1792d4718-2883-40aa-98c3-12c1a8868aa
name	User Account Administrator
objectId	00000003-0013-4c3f-98df-4bc77f409a31
objectType	Role
relatedId	File
relatedIdId	Fcd386e7-8e63-47db-81af-99c366c2881
type	ADRole

What is StormSpotter

Stormspotter creates an “attack graph” of the resources in an Azure subscription. It enables red teams and pentesters to visualize the attack surface and pivot opportunities within a tenant, and supercharges your defenders to quickly orient and prioritize incident response work.

Surveil

- Deep analytics tól
- Tekur meðal annars á
 - Öryggi (Zero Trust)
 - Identities
 - Network
 - Policies
 - Kostnaður
 - Configuration (stillingar og uppsetning)
 - Leyfismál



What is Surveil

Using Surveil's deep analytics and actionable insights, organisations can regain visibility and control over their Microsoft 365 and Azure environments. From opportunities to optimise licensing costs and solution adoption, to identifying security issues and duplicated functionality



Hvar skal byrja?

- *Náðu utan um núverandi stöðu á umhverfinu*
- *Búðu til framtíðar stefnu sem hefur allt fyrirtækið með að leiðarljósi*
- *Farðu í redesign sem passar við stefnuna*
- *Notaðu etv. Azure Landing Zones.*
- *Notaðu staðlaðar uppsetningar t.d. með Blueprints eða Terraform*

Takk fyrir



Grétar Gíslason



gretar@atmos.is



+354 860-5762