



# #GlobalAzure

## #CloudGenVerona

## @cloudgen\_verona

# Thanks to all the sponsors



## PREMIUM SPONSOR



## BASIC SPONSOR



CODICEPLASTICO





TOPIC

# **Funziona?! Allora non toccarlo,**

---

**ovvero l'analisi d'infrastruttura in esercizio.**

# Who I am



GIULIANO LATINI



@giulianolatini



[github.com/giulianolatini](https://github.com/giulianolatini)



[linkedin.com/in/giulianolatini/](https://linkedin.com/in/giulianolatini/)



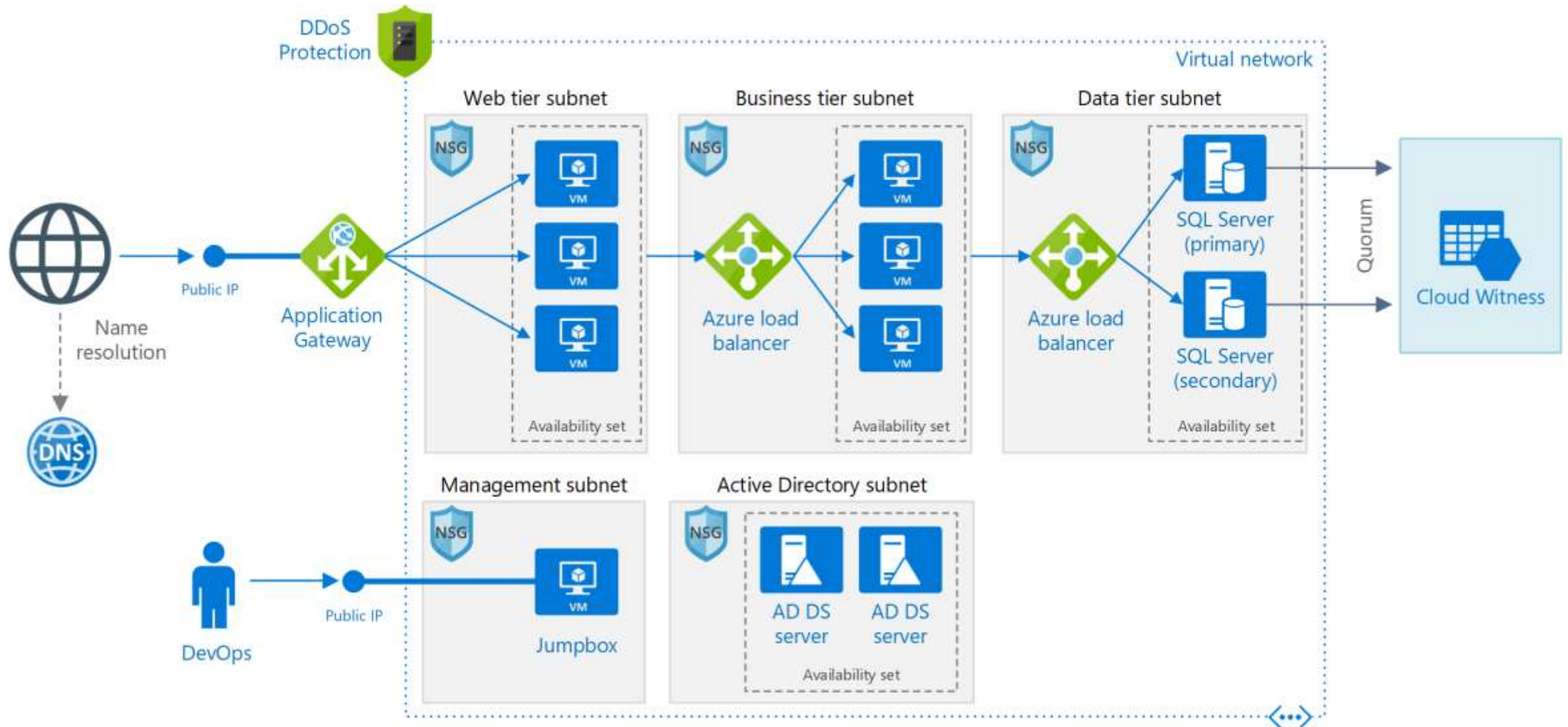
- Di cosa parliamo oggi?
- Come esplorare un'infrastruttura in Microsoft Azure
- Quali dati sono interessanti?
- Azure Resource Graph e Kusto Language
- Demo
- Cosa è installato nella VM
- Canali di accesso remote e consultazione dei pacchetti
- Demo
- Prospettive e soluzioni



“Power is nothing  
without control

Campagna Pirelli 1995

# Di cosa parliamo oggi?





- Manualmente/Documentazione ?
- Attraverso l'accesso <http://portal.azure.com/> ?
- Azure REST API ?
- Analisi dei Template ARM?
- Scripting ?
- Azure Resource Graph ?
- Excel/Power BI



# Quali dati sono interessanti?



- VMs
- Networking
- Risorse
- Images/Sku/Licensing
- States
- Storage location



## Azure Resource Graph

- Azure CLI (as an extension)
- Azure PowerShell Core (Az.ResourceGraph module)
- Azure PowerShell (AzureRM.ResourceGraph module)
- Azure Portal (“All Resources” and “Resource Graph Explorer” view)
- REST API
- Azure Cloud Shell



## Kusto Language

- Linguaggio Query
- Basato sul modello relazionale Tabelle/Colonne
- Operatori query per analisi complesse
- Query aggregabili tramite Pipeline
- In Azure Resource Graph non c'è supporto completo del linguaggio
- Analisi interattiva su BigData
- Es.: `where type =~ 'Microsoft.Compute/virtualMachines' | summarize count()`



# Azure Resource Graph

```
PowerShell v7.4.6
PS Azure:/
PS Azure:\> Enable-AzVMPSRemoting -Name 'vm-win-01' -ResourceGroupName 'azure-cloudshell-demo' -Protocol https -OsType Windows
PS Azure:/
PS Azure:\> Invoke-AzVMCommand -Name 'vm-win-01' -ResourceGroupName 'azure-cloudshell-demo' -ScriptBlock {get-service win*} -Credential $cred

Status      Name                DisplayName                                PSComputerName
-----
Running WinDefend           Windows Defender Antivirus Service         vmwin01.westus2.cloudapp.azure.com
Running WindowsAzureGuest... Windows Azure Guest Agent                  vmwin01.westus2.cloudapp.azure.com
Running WindowsAzureNetAg... Windows Azure Network Agent                vmwin01.westus2.cloudapp.azure.com
Running WindowsAzureTelem... Windows Azure Telemetry Service            vmwin01.westus2.cloudapp.azure.com
Running WinHttpAutoProxyS... WinHTTP Web Proxy Auto-Discovery Serv... vmwin01.westus2.cloudapp.azure.com
Running Winmgmt         Windows Management Instrumentation         vmwin01.westus2.cloudapp.azure.com
Running WinRM           Windows Remote Management (WS-Managem... vmwin01.westus2.cloudapp.azure.com

PS Azure:/
PS Azure:\>
```

# Canali di accesso remote



```
Windows PowerShell
PS C:\> Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object
DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize

DisplayName                                     DisplayVersion InstallDate
-----
Adobe AIR                                     3.8.0.1430
Microsoft .NET Framework 4 Client Profile     4.0.30319
Microsoft .NET Framework 4 Extended           4.0.30319
Microsoft Report Viewer Redistributable 2008 (KB971118)
Microsoft Visual J# 2.0 Redistributable Package - SE
Visual Studio 2005 Tools for Office Second Edition Runtime
Microsoft Office Professional Plus 2007        12.0.6612.1000
Wireshark 1.6.7 (32-bit)                       1.6.7
VMware vSphere Client 5.0                      5.0.0.34130    20130603
Microsoft .NET Framework 4 Extended           4.0.30319    20131024
Security Update for Microsoft .NET Framework 4 Extended (KB2416472) 1
Update for Microsoft .NET Framework 4 Extended (KB2468871) 1
```

```
Invoke-AzVMCommand -Name
gabcltSrv31 -ResourceGroupName
GAB2019TestLab01 -ScriptBlock
{get-service win*} -Credential
(get-credential)
```

```
ssh -T
giulianolattini@23.100.59.233
'dpkg-query -l'
```

```
root@ubuntu:~#
root@ubuntu:~# dpkg-query -f
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name Version Architecture Description
-----
ii accountsservice 0.6.40-2ubuntu10 amd64 query and manipulate user account information
ii acl 2.2.52-3 amd64 Access control list utilities
ii acpid 1:2.0.26-1ubuntu2 amd64 Advanced Configuration and Power Interface event daemon
ii adduser 3.113+nmu3ubuntu4 all add and remove users and groups
ii apache2 2.4.18-2ubuntu3.1 amd64 Apache HTTP Server
ii apache2-bin 2.4.18-2ubuntu3.1 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.18-2ubuntu3.1 all Apache HTTP Server (common files)
ii apache2-utils 2.4.18-2ubuntu3.1 amd64 Apache HTTP Server (utility programs for web servers)
ii apparmor 2.10.95-0ubuntu2.6 amd64 user-space parser utility for AppArmor
ii appport 2.20.1-0ubuntu2.4 all automatically generate crash reports for debugging
ii appport-symptoms 0.20 all symptom scripts for appport
ii apt 1.2.15ubuntu0.2 amd64 commandline package manager
ii apt-transport-https 1.2.15ubuntu0.2 amd64 https download transport for APT
ii apt-utils 1.2.15ubuntu0.2 amd64 package management related utility programs
ii at 3.1.18-2ubuntu1 amd64 Delayed job execution and batch processing
ii base-files 9.4ubuntu4 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.39 amd64 Debian base system master password and group files
ii bash 4.3-14ubuntu1 amd64 GNU Bourne Again Shell
ii bash-completion 1:2.1-4.2ubuntu1 all programmable completion for the bash shell
```



# Canali di accesso remote e consultazione dei pacchetti



```
Windows PowerShell
PS C:\> Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object
DisplayName, DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize

DisplayName                                DisplayVersion InstallDate
-----
Adobe AIR                                3.8.0.1430
Microsoft .NET Framework 4 Client Profile 4.0.30319
Microsoft .NET Framework 4 Extended       4.0.30319
Microsoft Report Viewer Redistributable 2008 (KB971118)
Microsoft Visual J# 2.0 Redistributable Package - SE
Visual Studio 2005 Tools for Office Second Edition Runtime
Microsoft Office Professional Plus 2007    12.0.6612.1000
Wireshark 1.6.7 (32-bit)                  1.6.7
VMware vSphere Client 5.0                 5.0.0.34130    20130603
Microsoft .NET Framework 4 Extended       4.0.30319      20131024
Security Update for Microsoft .NET Framework 4 Extended (KB2416472) 1
Update for Microsoft .NET Framework 4 Extended (KB2468871) 1
```

Get-ItemProperty  
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\\* | Select-Object  
DisplayName, DisplayVersion,  
Publisher, InstallDate | Format-Table  
-AutoSize

dpkg-query -l

```
root@ubuntu:~#
root@ubuntu:~# dpkg-query -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                      Version                Architecture           Description
+++-+-----+-----+-----+-----+
ii accountsservice            0.6.40-2ubuntu10      amd64                  query and manipulate user account information
ii acl                         2.2.52-3              amd64                  Access control list utilities
ii acpid                       1:2.0.26-1ubuntu2     amd64                  Advanced Configuration and Power Interface event daemon
ii adduser                     3.113+nmu3ubuntu4     all                    add and remove users and groups
ii apache2                     2.4.18-2ubuntu3.1     amd64                  Apache HTTP Server
ii apache2-bin                 2.4.18-2ubuntu3.1     amd64                  Apache HTTP Server (modules and other binary files)
ii apache2-data                 2.4.18-2ubuntu3.1     all                    Apache HTTP Server (common files)
ii apache2-utils                2.4.18-2ubuntu3.1     amd64                  Apache HTTP Server (utility programs for web servers)
ii apparmor                    2.10.95-0ubuntu2.6    amd64                  user-space parser utility for AppArmor
ii appport                     2.20.1-0ubuntu2.4     all                    automatically generate crash reports for debugging
ii appport-symptoms            0.20                  all                    symptom scripts for appport
ii apt                          1.2.15ubuntu0.2       amd64                  commandline package manager
ii apt-transport-https         1.2.15ubuntu0.2       amd64                  https download transport for APT
ii apt-utils                    1.2.15ubuntu0.2       amd64                  package management related utility programs
ii at                           3.1.18-2ubuntu1       amd64                  Delayed job execution and batch processing
ii base-files                   9.4ubuntu4            amd64                  Debian base system miscellaneous files
ii base-passwd                  3.5.39                amd64                  Debian base system master password and group files
ii bash                         4.3-14ubuntu1         amd64                  GNU Bourne Again SHell
ii bash-completion              1:2.1-4.2ubuntu1     all                    programmable completion for the bash shell
```



# Lista del Software Installato





- Interroghiamo l'infrastruttura
- Inspezionabilità per soluzioni Infrastructure as Code
- Esportabilità verso Excel/Power BI
- Rilevamento di variazioni per infrastruttura
  
- Documentazione?
- Dashboard di stato per live monitor?
- Query pinnabili sulla dashboard Azure ?



- [Azure Resource Graph Documentation - Tutorials, API Reference](#)
- [Reference - Azure Data Explorer - Kusto Query Language](#)
- [Getting started with Kusto - Azure Data Explorer](#)
- [Kusto Tools - Azure Data Explorer](#)
- [Documentazione di Resource Manager in Azure - Esercitazioni, esempi, informazioni di riferimento e risorse](#)
- [Saving time with Azure Resource Graph](#)
- [Explore Azure Resources with Resource Graph](#)



- [MicrosoftDocs/azure-docs/articles/governance/resource-graph/](#)
- [MicrosoftDocs/azure-docs/articles/governance/resource-graph/samples/](#)
- [Azure Resource Graph Introduction](#)
- [Explore Azure Resources With Resource Graph - DZone Cloud](#)
- [Azure Resource Graph: How many CPU cores are used](#)
- [Top 10 PowerShell Script to check the Windows Service on remote server - OnClick360](#)
- [Remoting into Azure ARM Virtual Machines using Powershell](#)
- [PowerShell Basics: Connecting to VMs with Azure PSRemoting](#)



- [Check Azure VM status with PowerShell](#)
- [Configure PowerShell remoting for Azure VMs - Powershellbros.com](#)
- [Enable PowerShell Remoting to an Azure Virtual Machine, without Domain Membership | Azure | SignalWarrant.com - Practical PowerShell for Humans](#)
- [Use PowerShell to Quickly Find Installed Software | Scripting](#)
- [Use PowerShell to Find Installed Software | Scripting](#)
- [How to Create a List of Your Installed Programs on Windows](#)



## Abilita Resource Graph

- PowerShell: `Install-Module -Name AzureRm.ResourceGraph -AllowPrerelease`
- PowerShell: `Install-Module -Name Az -AllowClobber`
- CLI: `az extension add --name resource-graph`



## Esempi di Query

### Powershell

```
Search-AzGraph -Query "project name, type, location | order by name asc"
```

```
search-AzureRmGraph -Query "where type =~ 'Microsoft.Compute/virtualMachines' and name == 'gabcltSrv31' "
```

### CLI

```
az graph query -q "project name, type, location | order by name asc"
```

```
az graph query -q "where type =~ 'Microsoft.Compute/virtualMachines' | project name, type, location | order by name asc" --output tsv |  
out-file numberofcores.csv
```

```
az graph query -q "where type =~ 'Microsoft.Compute/virtualMachines' and name == 'gabcltSrv31' "
```

```
az graph query -q "where type =~ 'Microsoft.Compute/virtualmachines' and properties.hardwareProfile.vmSize matches regex 'Standard_DS[0-9]*_v2' | project name"
```



## Accesso VM

### Abilitazione Remoting

```
Enable-AzVMPSRemoting -Name 'gabcltSrv31' -ResourceGroupName 'GAB2019TestLab01' -Protocol https -OsType Windows  
Enable-AzVMPSRemoting -Name 'gabwebSrv32' -ResourceGroupName 'GAB2019TestLab01' -Protocol https -OsType Windows  
Enable-AzVMPSRemoting -Name 'gabwebSrv21' -ResourceGroupName 'GAB2019TestLab01' -Protocol ssh -OsType Linux
```

### Connessione con Prompt

```
Enter-AzVM -name 'gabwebSrv32' -ResourceGroupName 'GAB2019TestLab01' -Credential (get-credential)  
Enter-AzVM -name 'gabcltSrv31' -ResourceGroupName 'GAB2019TestLab01' -Credential (get-credential)  
  
choco install vscode  
  
ssh giulianolatini@23.100.59.233
```





## Lista Software Installati

```
Invoke-AzVMCommand -Name gabcltSrv31 -ResourceGroupName GAB2019TestLab01 -ScriptBlock {get-service win*} -Credential (get-credential)

Invoke-AzVMCommand -Name 'gabcltSrv31' -ResourceGroup 'GAB2019TestLab01' -ScriptBlock {Get-ItemProperty
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-
Table -AutoSize} -Credential (get-credential)

$cred = get-credential

Invoke-AzVMCommand -Name 'gabcltSrv31' -ResourceGroup 'GAB2019TestLab01' -ScriptBlock {get-service win*} -Credential $cred

Invoke-AzVMCommand -Name 'gabcltSrv31' -ResourceGroup 'GAB2019TestLab01' -ScriptBlock {Get-ItemProperty
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-
Table -AutoSize} -Credential $cred

ssh -T giulianolatini@23.100.59.233 'dpkg-query -l'
```





## Conclusione

```
$cred = get-credential

$machine = az graph query -q "where type =~ 'Microsoft.Compute/virtualMachines' and name == 'gabcltSrv31' | project name " --output tsv

foreach ($computer in $machine) { Invoke-AzVMCommand -Name $computer -ResourceGroup GAB2019TestLab01 -ScriptBlock {Get-ItemProperty
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-
Table -AutoSize} -Credential $cred }

az graph query -q "where type =~ 'Microsoft.Compute/virtualMachines' and name == 'gabcltSrv31' | project name " --output tsv | foreach {
Invoke-AzVMCommand -Name $_ -ResourceGroup GAB2019TestLab01 -ScriptBlock {Get-ItemProperty
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Format-
Table -AutoSize} -Credential (get-credential) }
```



# Thanks

Questions?



[github.com/giulianolatini](https://github.com/giulianolatini)



[giulianolatini](https://twitter.com/giulianolatini)



[linkedin.com/in/giulianolatini/](https://linkedin.com/in/giulianolatini/)