delaware

connecting SAP RISE through Connectivity HUB

2-day workshop

Providing best practices on a Connectivity HUB:

- VNET peering to SAP RISE with full connectivity from RFC-1918
- Connection to the HUB based on Microsoft PaaS components or NVA
- Possible additional services with AVD

As an SAP technology partner with a wide background of executed projects, **delaware** has been part of implementations where has supported its clients to:

Solve and improve communication problems towards SAP

Evaluate scenarios where latency can be so high that affects the productivity of the environment

Improve environments in which long times are required to obtain extra connectivity, avoiding the effects of a connection without the minimum standard.

Goal

- Recognition of the current organization landscape
- Discuss and align the stakeholders involved in the solution with price-quality ratio, guaranteeing security and manageability throughout the cycle.
- Provide additional information about additional non-SAP Azure services

SAP offers connectivity towards SAP RISE, based on:

- **Public Access**
- **Virtual Private Networks**
- **ExpressRoute**
- **VNET Peering (only within Microsoft Azure)**

The workshops

RISE WITH SAP

Day 1

Getting to know the landscape

- Get knowledge on the current customer landscape
- How can you secure access SAP RISE
- Do's and Don'ts
- Discuss PaaS vs NVA
- Extra Services in the Connectivity HUB

Day 2

Day 2: In-depth sessions for analysis, preparation and report

Preparation of the technical information collected and presented as a report covering each of the topics of both workshops.

The workshops are planned on a period of 2 days. After the first workshop, in-depth sessions and automated security improvements will be identified and planned.

we commit. we deliver.

delaware.pro

> “
> Average total cost of a data breach is
> **$3.86 million, nearly 40% from lost business**
> ”

Source: Cost of a Data Breach Report 2020 - Ponemon Institute/IBM

But, how can **delaware** support your organization in this process?

connecting SAP RISE through Connectivity HUB

Standardize communication between SAP and the Internet.

Efficiently control traffic within on-premises facilities such as in Microsoft Azure

Correct use of network security groups (NSG)

Communication within the SAP virtual network evaluating type of workload and environment to which it belongs

Control any communication flow between SAP in Azure and on-premises environments by routing everything through the Firewall.

Communication within the same region or between other regions is routed through the Azure firewall.

Microsoft Partner

Microsoft

Gold Security
Gold Cloud Business Applications

SAP Gold Partner