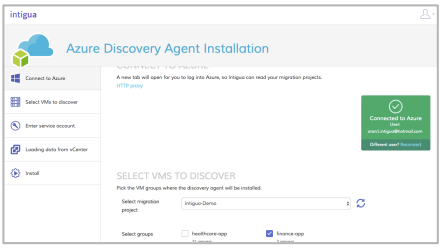
intigua | Simplifying Cloud Server Automation



Migrate To Azure Quickly And Stay in Control

HIGHLIGHTS

Simplify and accelerate the Discovery phase of migration with quick, controlled dependency agent deployment.

Simplify and accelerate the Migrate phase with quick, controlled deployment of ASR.

Native Linux support, no need for complex SCCM setup.

Use of network management ports is strictly optional.

Enjoy advanced Azure and third-party server management services after migration with quick agent deployment and automation.

Use policies and RBAC for advanced scenarios.

You need to get those big, money-making apps into the cloud, ASAP. But how do get it done without breaking critical apps?

The discover / migrate / manage workflow takes you safely through the migration process. First, you need to understand which servers make up your application, and what their dependencies on other services are. Intigua for Azure Migrate lets you quickly set up the Azure Migrate agents that make full dependency mapping a snap. No complex SCCM setup is necessary, and Linux servers can be discovered just as easily as Windows ones. No network tweaks are needed either – as long as Intigua has access to your vCenter, it can install agents even to VMs that live in isolated networks.

When ready to migrate, Intigua for Azure Site Recovery lets you set up the ASR agent just as quickly. Again, no extra preparations are needed in terms of networking, SCCM or Linux setup. If you've already used Intigua to achieve quick dependency mapping, adding ASR is trivial.

Once you migrate to Azure, a whole new set of management services is available to you from Microsoft. But how do you ensure the agents for these services get installed and maintained on your servers? Intigua for Azure Pro lets you work with Azure services such as Backup, Security & Compliance, Protection & Recovery and more. Use Intigua alone or integrated with Azure Automation and Powershell, to achieve simple server automation that just works.

Intigua also lets you tackle more advanced scenarios with ease. Set up multiple vCenter or Azure accounts, and use policies to automatically manage servers according to you guidelines. Use remote execution and diagnostic options, along with role-based access control (RBAC), to troubleshooet common issues while keeping tight limitations on VM access.