Microsoft® Azure in the data center

HPE ProLiant for Microsoft Azure Stack offers an on-premises instance of a Microsoft Azure® Stack, which is an on-premises extension of Microsoft Azure public cloud. Azure Stack is fully compatible with Azure development and deployment tools.

It is co-engineered by Hewlett Packard Enterprise and Microsoft, and incorporates compute, storage, and networking in an Azure on-premises instance. HPE ProLiant for Microsoft Azure Stack enables a hybrid cloud solution that is fully consistent with Azure public cloud services. This approach delivers the speed, agility, and simplicity of a public cloud with the cost-effectiveness, flexibility, and data sovereignty characteristics of an on-premises cloud.

Enterprise challenges

HPE ProLiant for Microsoft Azure Stack has proven itself in the enterprise. However, some users wish to take the solution even further by addressing challenges they face, including achieving high availability (HA) for the solution stack and improving security countermeasures. For example, Azure Stack can be vulnerable to volumetric attacks, which can affect performance and reliability. As is, the stack also requires its own dedicated login. This requirement creates potential security risks while reducing end-user productivity.

The F5 solution

F5 Networks, whose mission is based on making sure applications are available and secure, has worked with HPE to develop a solution to augment the capabilities of HPE ProLiant for Microsoft Azure Stack. F5 works with the world’s leading technology companies on strengthening manageability and security while ensuring faster and more successful deployments. This Azure Stack solution is the latest in a long, collaborative partnership between F5 and HPE. Its joint customers benefit from the integration and interoperability resulting from such a close collaboration.

Solution overview

The F5 solution has been validated for HPE ProLiant for Microsoft Azure Stack for HA. It works primarily by acting as a load balancer between two or more Azure Stack instances. The F5 solution runs on a virtual machine (VM) on a hypervisor, where it can allocate between various tenant workloads on each stack. The VM connects with top-of-rack (ToR) switches and baseboard management controllers (BMCs) on each stack through a border device on each stack.

Load balancing

With this architecture, the F5 solution can balance loads between each of the HPE ProLiant for Microsoft Azure Stack instances. The load balancing occurs between Layer 4 and Layer 7 of the networks, guided by in-band monitoring.
Incoming traffic is balanced between applications and databases to ensure reliability and performance.

F5 also offloads decryption and encryption of traffic workloads. By doing encrypt/decrypt in front of Azure Stack, the F5 solution enables better application performance and a more efficient use of resources. A similar effect results from moving read/write operations to a separate, synchronized Azure Stack in a different location.

Users put the F5 solution's load-balancing capabilities to work setting up failover for critical systems. By keeping two or more Azure Stack instances in sync, F5 can manage instant failover if there is an outage on one of them. For example, a retailer might set up the back end of its point of sale (POS) system on a pair of Azure Stacks synchronized by F5 load balancing. They do this because an outage in the POS system will hurt revenue and customer experience. With the F5 solution in place, a POS outage will have virtually no impact on business operations.

**Supplementary web application firewall**

The F5 solution for HPE ProLiant for Microsoft Azure Stack supplements the stack's built-in security countermeasures. The solution's web application firewall offers additional protection against volumetric-type attacks that can overload applications running on the stack. The same functionality can also detect and prevent exfiltration of data from the Azure Stack. As has been observed in many of the worst data breaches, the exfiltration of data over long periods of time, which often goes unnoticed, compounds the impact of the breach. F5 mitigates this risk.

**Single sign-on (SSO)**

Microsoft Azure Stack requires a separate login for users. This requirement has the potential to affect ease of use and productivity. The F5 solution addresses this issue by enabling federated identity management (FIM). Applied to Microsoft Azure Stack, FIM makes it possible for users to log in once and then be authenticated and authorized to access applications on the stack.

This SSO capability will work between public and on-premises instances of Azure, as well as between Azure Stack and virtually any other application in the enterprise. In the POS example, for instance, an admin could sign on to the network and access the retailer's email server, accounting system, and POS system all with one set of login credentials.

**Customer benefits**

Applying the F5 load balancing solution to HPE ProLiant for Microsoft Azure Stack confers a number of benefits to the enterprise. These include:

- Multiple HA scenarios:
  - Application HA—Making applications highly available across the cloud and on-premises, or between multiple Azure Stack instances
  - Localized HA—Allowing two or more Azure Stack instances at the same site to act as failover instances for each other
  - Multi site/multi region HA—Bridging Azure Stack instances deployed in multiple data centers, including deployments in separate geographic regions
- Improved security posture—Protecting applications and data on Azure Stack against volumetric attacks and exfiltration contributes to an overall improvement in an organization's security posture
- Improved end-user productivity—Leveraging SSO, users of applications on Azure Stack can work more productively

Learn more at [hpe.com/cloud/azure-stack](http://hpe.com/cloud/azure-stack)