Microsoft Azure - Starter Kits for Partners

Architecture

Site Recovery

Last Update: 22 September 2015





**MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2014 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Overview 4](#_Toc430733324)

[Service Description 5](#_Toc430733325)

[Protecting to Azure 5](#_Toc430733326)

[Protection to Secondary Site 6](#_Toc430733327)

[Strategy and Architecture 7](#_Toc430733328)

[Architecture Details 7](#_Toc430733329)

[1a - Protecting to Azure 8](#_Toc430733330)

[1b – Migrating to Azure 9](#_Toc430733331)

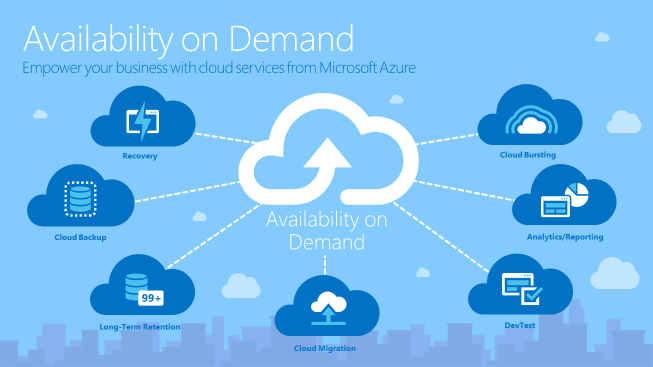
[02 – Protecting to a Secondary Site 10](#_Toc430733332)

[03 – Protecting VMWare to Azure 11](#_Toc430733333)

Architecture for Azure Site Recovery

# Overview

Availability has been traditionally viewed as recovery in the cloud, but Microsoft breaks this mold and sets a new standard with Availability on Demand. Once a connection from your datacenter to Azure is established, your servers are replicated, much like a traditional recovery or backup solutions. With your data now in Azure, you not only have the safety net of being able to leverage Azure as a secondary site in a time of need, but you also have unfettered access to the robust compute and storage capacity of Azure. Since your data is already in Azure, standing up a replicated workload in Azure for DevTest, or assigning a larger Azure template to provide additional compute capacity is as simple as a few clicks – without affecting your on premises production workload. Just as easy as getting your data into Azure, bring it back on premises in the same manner, even if a physical server or VMware virtual machine.



The purpose of this document is to describe the Recovery and Cloud Migration scenarios from Availability on Demand model. In the next sections, you will see the details about the scenarios for Disaster Recovery and Migration to Microsoft Azure by using Azure Site recovery.

# Service Description

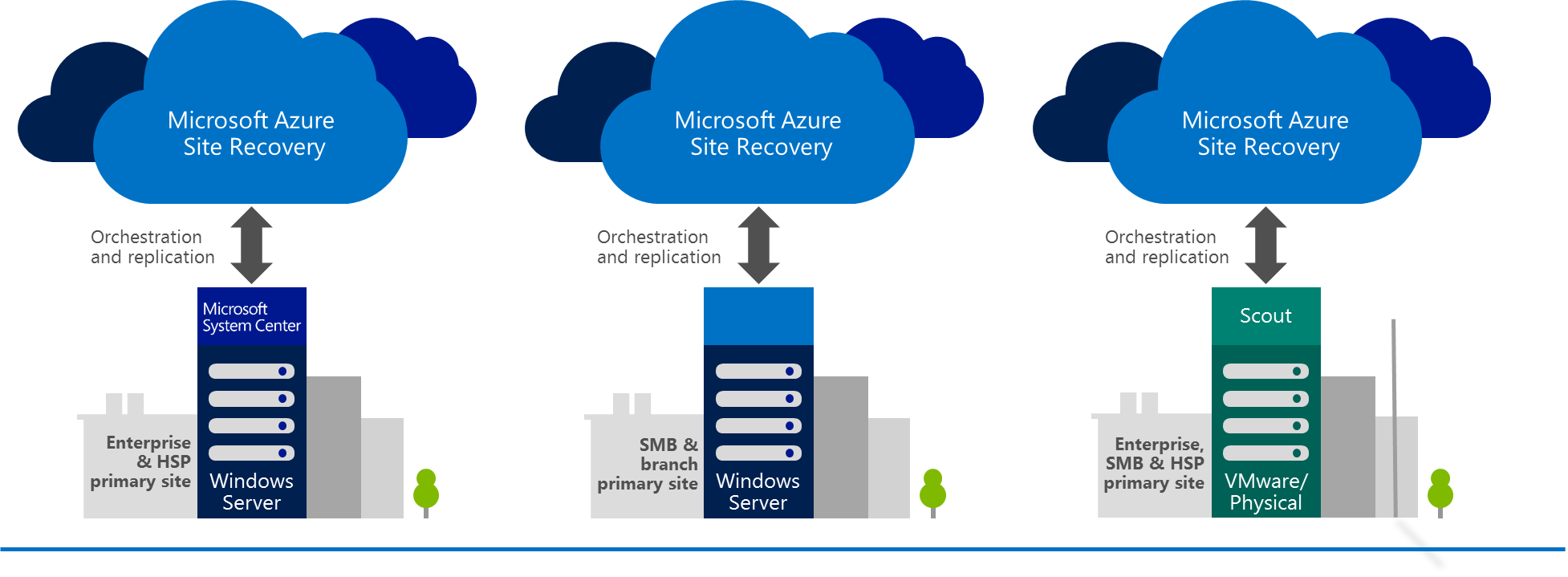
The Site Recovery service contributes to a robust business continuity and disaster recovery (BCDR) solution that protects your on-premises physical servers and virtual machines by orchestrating and automating replication and failover to Azure, or to a secondary on-premises datacenter.

See below the high-level architecture for the two protection options: Protecting to Azure or Protecting to Secondary Site.

## Protecting to Azure

Protection to Azure is necessary when customer does not have a secondary site to replicate and protect its production environment. In this strategy, Microsoft Azure will:

* Orchestrate and automate the failover and protection between locations;
* Be the target for the replication of protected resources;

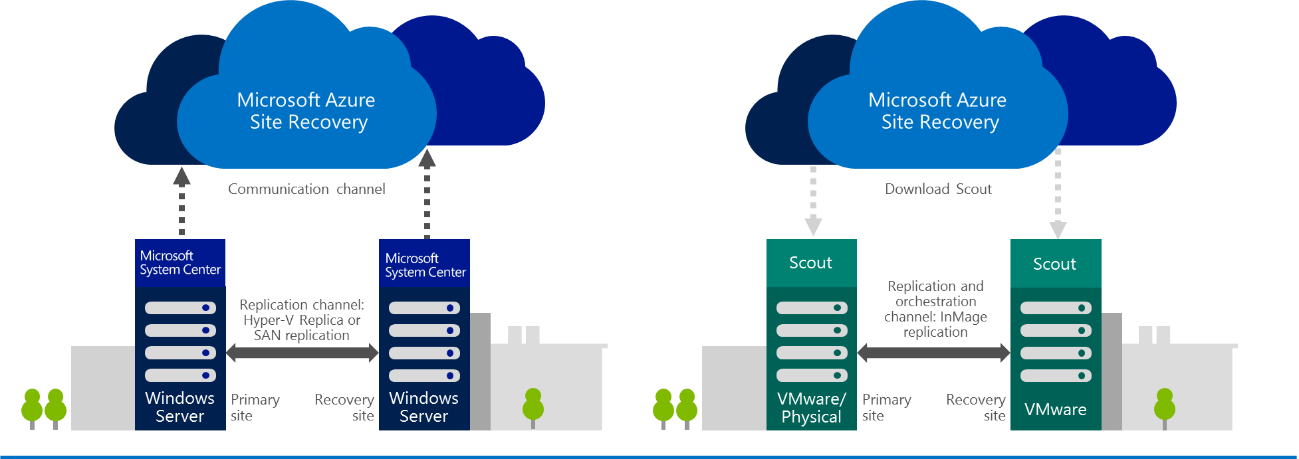


These possible variations can be applied according customers’ infrastructure:

|  |  |
| --- | --- |
|  | Protect cloud from System Center VMM to Microsoft Azure; |
|  | Protect virtual machines from Hyper-V host to Microsoft Azure; |
|  | Protect physical or VMWare virtual machines to Azure; |

## Protection to Secondary Site

Azure Site Recovery also provides the ability of protecting customers’ critical workloads to a secondary location. In this strategy, Microsoft Azure will orchestrate and automate failover and protection between locations, replication target will be always the secondary location owned by the customer.



These possible variations can be applied according customers’ infrastructure:

|  |  |
| --- | --- |
|  | Protect VMM cloud to a secondary VMM with network replication; |
|  | Protect VMM cloud to a secondary VMM with SAN replication; |
|  | Protect physical or VMWare cloud to a secondary VMWare cloud; |

# Strategy and Architecture

Azure Site Recovery capabilities allows you not only to protect your customers’ environment, but also allows you to:

* Migrate to Azure IaaS capabilities;
* Deploy a Dev/Test environment;
* Handle high-demanding periods, also known as Cloud-Bursting;
* Create high performing environments for specific tasks;

Even though we can apply many approaches based on business scenarios, two main strategies act as a foundational base: Protection and Migration. When you engage in an Azure Site Recovery project, you can choose to:

* Protect primary environment by creating a replica to Azure or a secondary location, which will be the core of you Disaster Recovery Solution;
* After protecting customers’ environment, you can trigger a planned-failover, which will shut down all protected on-premises infrastructure and start Azure virtual machines according your plan. This is a migration scenario.

## Architecture Details

Based on the most common and relevant strategies for our customers and partners four main scenarios were designed and are available below. Additionally, these variations will affect what is the consumption of Azure services and consequently, the pricing for the entire solution.

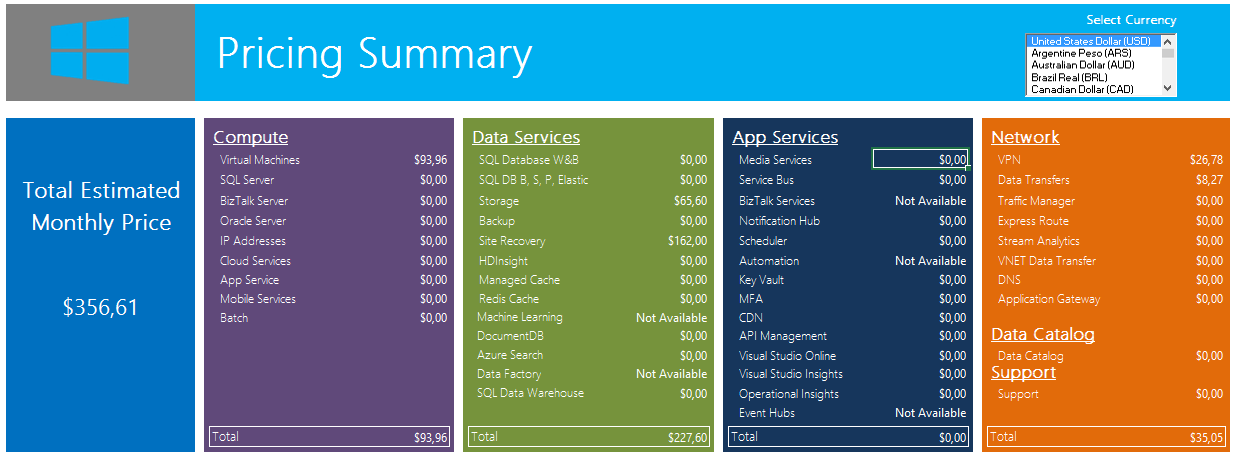
### 1a - Protecting to Azure

This diagram represents the protection of an on-premise workload to Microsoft Azure.



The following services are represented in the diagram and compose solution costs:

* 3 instances protected to Azure by Azure Site recovery;
* Virtual Machines
  + 744 hours per month for infrastructure components, such as Active Directory;
  + 25 hours per month based on availability estimation and SLA of 95% for protected workloads;
* Geo-Redundant and Locally-Redundant Storage for protected workloads and infrastructure components;
* Storage Transactions
* 744 hours of VPN gateway for hybrid communication;
* Data egress from Azure



More details available at: **5 - Cost Estimator - Scenario 1a - Protecting to Azure.xlsm**

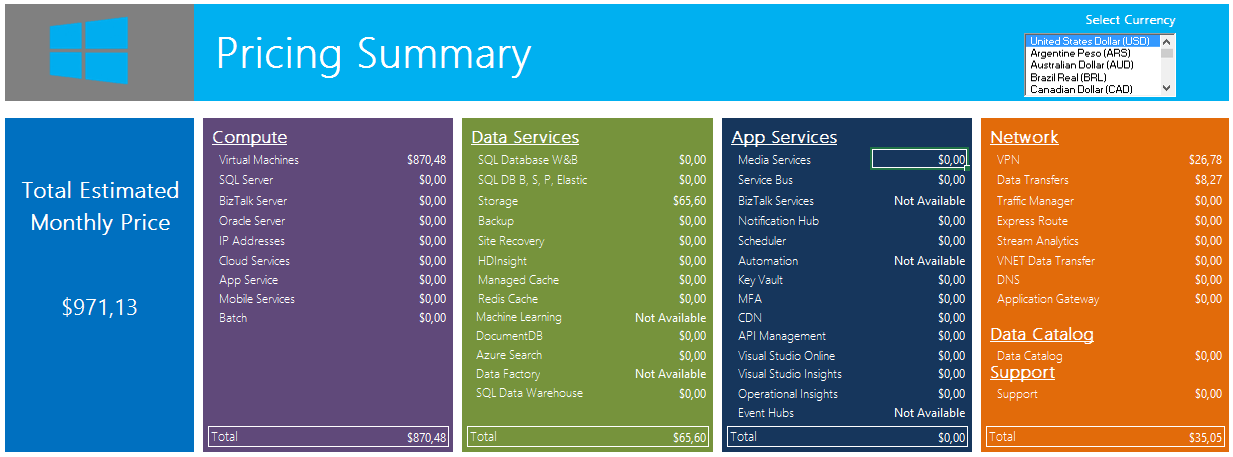
### 1b – Migrating to Azure

This diagram represents the migration of an on-premise workload to Microsoft Azure.



The following services are represented in the diagram and compose solution costs:

* 3 instances protected to Azure by Azure Site recovery. In case migration occurs within 31 days, there are no costs for ASR protection;
* Virtual Machines
  + 744 hours per month for all virtual machines;
* Geo-Redundant and Locally-Redundant Storage for protected workloads and infrastructure components;
* Storage Transactions
* 744 hours of VPN gateway for hybrid communication;
* Data egress from Azure



More details available at: **5 - Cost Estimator - Scenario 1b - Migrating to Azure.xlsm**

### 02 – Protecting to a Secondary Site

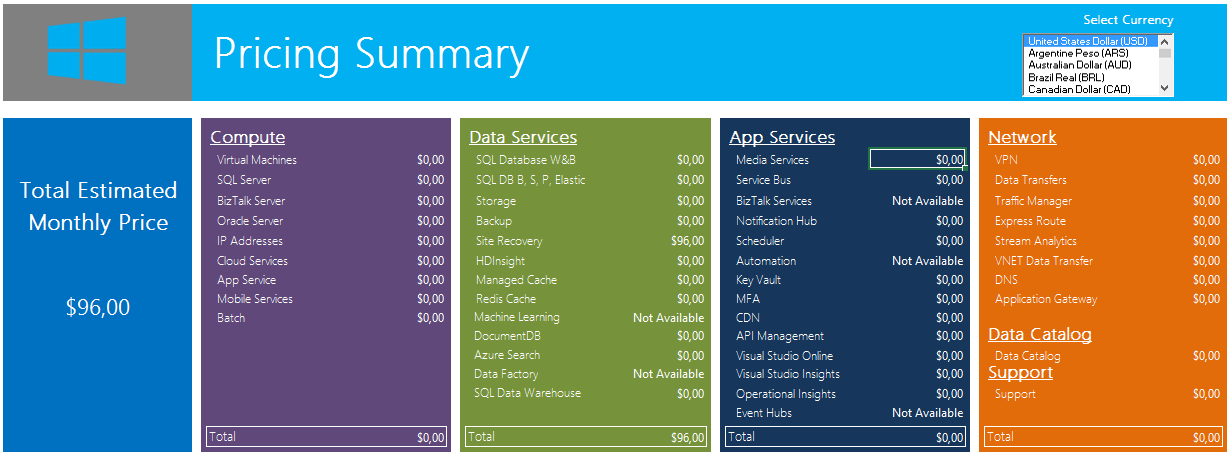
This diagram represents the protection of workloads from primary to secondary location. Replication in this case is handled by the customer. Azure is responsible only for orchestrating and automating the recovery.

This diagram and cost estimation applies to:

* VMM protection with network replication or SAN replication;
* VMWare and physical machines protection;

 The following services are represented and compose solution costs:

* 6 intances protected to customer-owned sites;



More details available at: **5 - Cost Estimator - Scenario 02 - Protecting to Secondary Site.xlsm**

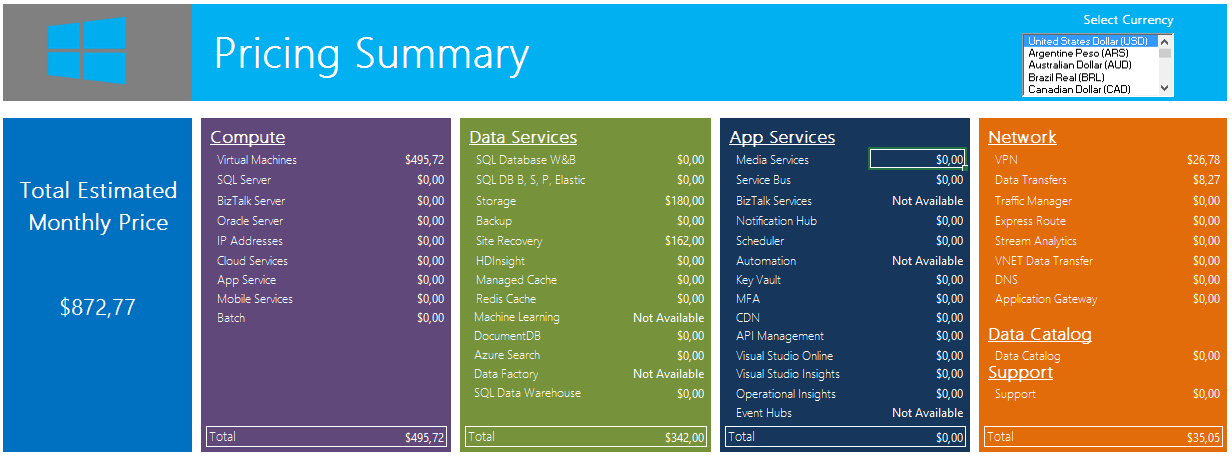
### 03 – Protecting VMWare to Azure

This diagram represents the protection of an on-premise VMWare workload to Microsoft Azure.



The following services are represented in the diagram and compose solution costs:

* 3 instances protected to Azure by Azure Site recovery;
* Virtual Machines
  + 744 hours per month for infrastructure components, such as Active Directory and ASR Scout components, required by VMWare and physical protection;
  + 25 hours per month based on availability estimation and SLA of 95% for protected workloads;
* Geo-Redundant and Locally-Redundant Storage for protected workloads and infrastructure components;
* Storage Transactions
* 744 hours of VPN gateway for hybrid communication;
* Data egress from Azure



More details available at: **5 - Cost Estimator - Scenario 03 - Protecting VMWare to Azure.xlsm**