ToDo

- nothing

Windows Azure

Базовые роли

В этом модуле:

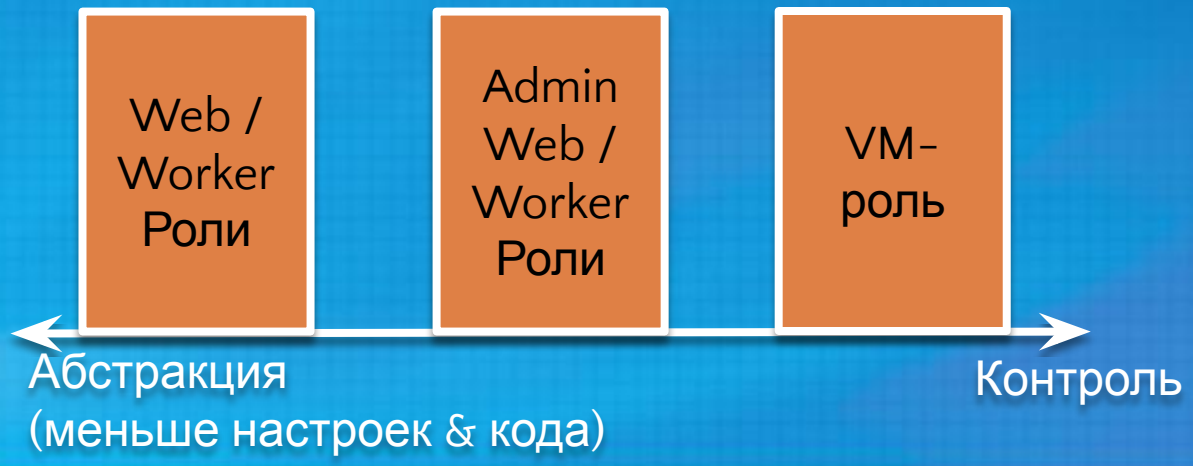
- Что такое роль?
- Назначение каждой роли
- Базовая конфигурация ролей.
- Локальная отладка.

Роли и экземпляры

- Роли определяются в сервисной модели
  - Можно определить одну или более ролей на сервис
  - Определение роли содержит
    - Размер виртуальной машины
    - Endpoints для коммуникации
    - Локальные ресурсы хранилища
    - Etc…
- Каждая роль выполняется на одном или более экземплярах (до 20 на подписку))
  - Экземпляр роли: код, конфигурация и локальные данные. Разворачивается в отдельную виртуальную машину

Сравнение типов ролей

- *Web-роль*: Роль, основанная на ***IIS***
- *Worker-роль*: Роль, основанная на выполняемом коде (можно создать собственный веб-сервер, управлять базой данных, …)
- *VM-роль*: Роль **виртуальной машины**.
  - Windows-сервисы, назначенные задания, etc.
  - **Вы настраиваете и обслуживаете ОС.**



Роли сервисов вычислений

Web и Worker-роли

Операционная система обеспечивается Microsoft

Обновление осуществляется Microsoft

- Клиентам предоставляются администраторские права, код работает под аккаунтом с минимальными привилегиями
- Полный или частичный уровень доверия .NET (по умолчанию полный)
- Полный доступ к локальной файловой системе, но нет постоянного локального хранения

VM-роль

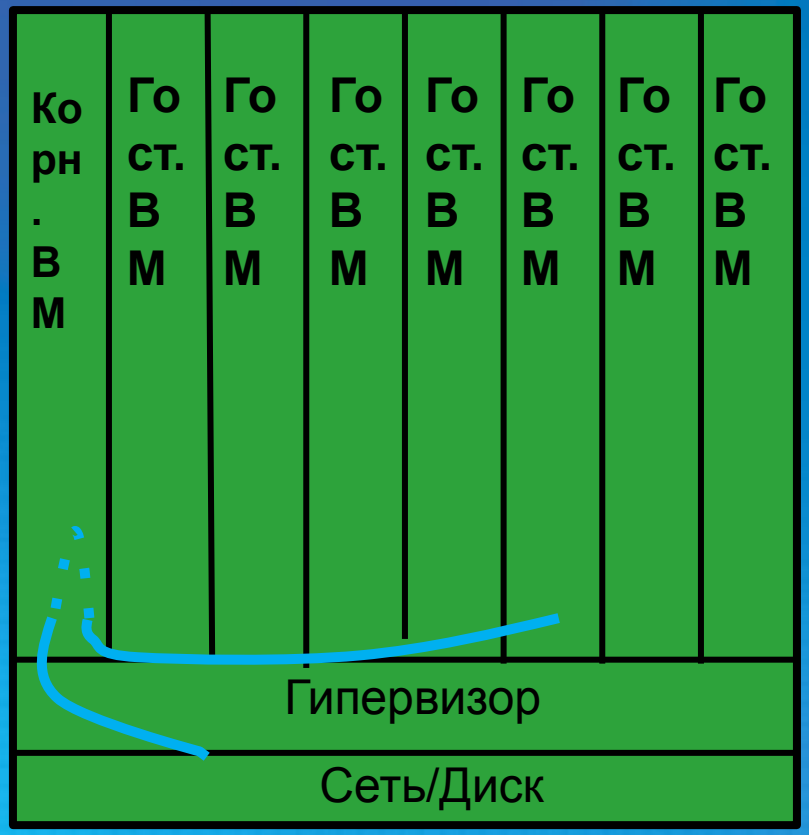
Операционная система обеспечивается клиентом

Обновление осуществляется клиентом

- Клиентам предоставляются администраторские права,
- Отсутствие поддержки
- Лицензирование ОС включено в цену использования Windows Azure

Безопасность сервисов

Гипервизор и «Песочница»

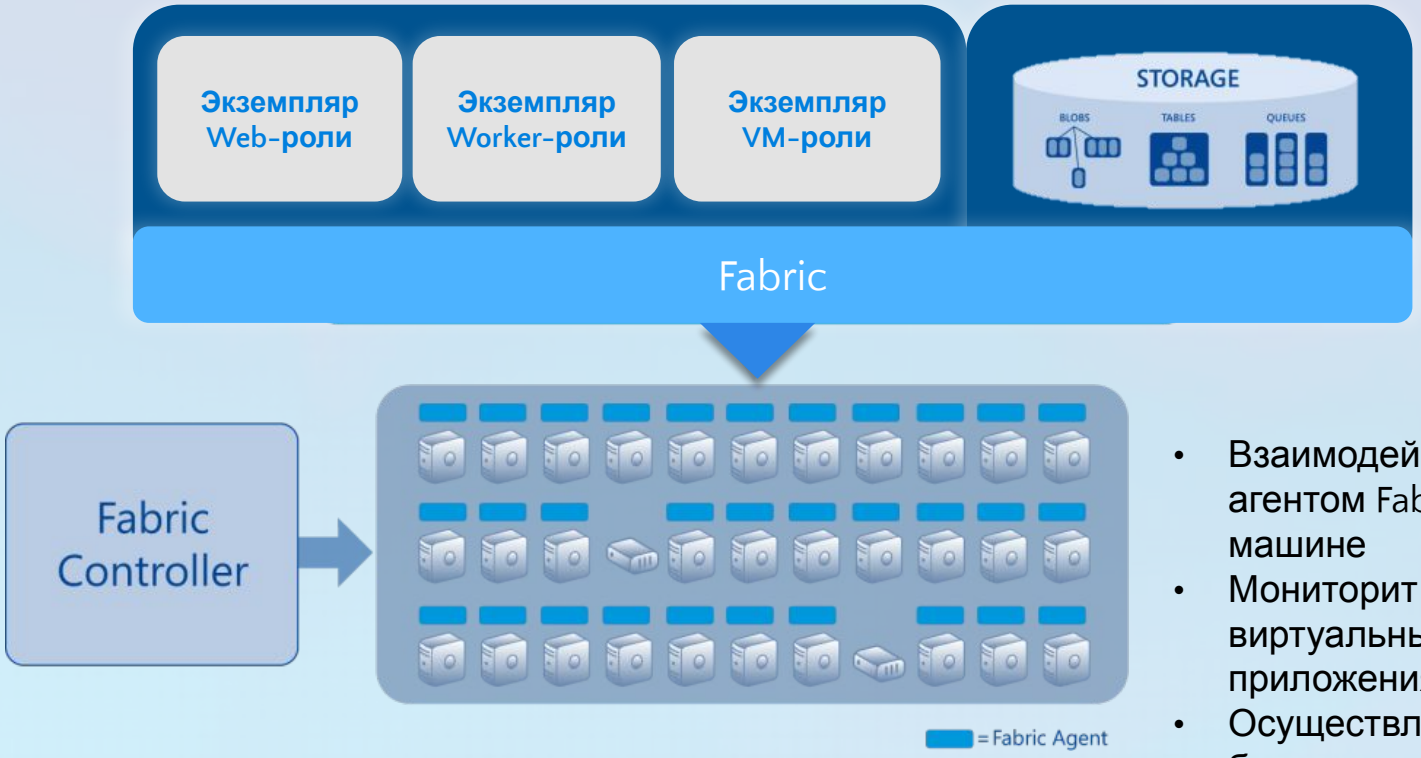


- 1, 2, 4 или 8 CPU, до 14Гб ОЗУ
- «Обрезанная» версия Windows Server 2008
- Три виртуальных жестких диска
- Ограниченное количество драйверов устройств
- Ограничения подключения брандмауэром

Гипервизор на основе Hyper-V

- Клиентский код выполняется на выделенных виртуальных машинах
- Виртуальные машины изолированы гипервизором на основе Hyper-V
- Все сетевые и дисковые операции контролируются «корневой» виртуальной машиной

Fabric-контроллер



- Взаимодействует с агентом Fabric на каждой машине
- Мониторит все виртуальные машины, приложения и экземпляры
- Осуществляет балансировку нагрузки, установку контрольных точек и восстановление

Изолированность в Windows Azure

- Не основана на безопасности Windows
  - Основана на безопасности, обеспечиваемой гипервизором, сети и выставленных сетевых и дисковых драйверов
  - Поверхность атаки минимизирована уменьшением количества команд и поддержки небольшого количества устройств
- Процессорные ядра выделены для конкретных виртуальных машин для предотвращения атаки по сторонним каналам (side-channel attack)
- Гостевые диски – файлы VHD, находящиеся в файловой системе ОС корневой виртуальной машины
- Гипервизор и ОС корневой виртуальной машины используют фильтры пакетов для блокировки спуфированного или нежелательного трафика

Безопасность при управлении сервисом

- Клиент создаёт подписку используя аккаунт Live ID
- Сервисы и аккаунты хранилища управляются либо с помощью Live ID, либо Service Management API (с использованием сгенерированных пользователем пар публичный/приватный ключ)
- Fabric-контроллер управляет и обновляет вычислительные и узлы хранения
  - Экземпляры Fabric-контроллера работают на отдельном от сервисов оборудовании
  - Коммуникации между Fabric-контроллерами и узлами аутентифицируются и шифруются SSL

Что такое Web-роль?

Web-роль – работающий под управлением IIS веб-сайт или сервис.

- Поддерживает HTTP, HTTPS и сертификаты
- Azure автоматически распределяет нагрузку на Web-роли
- Может быть только внутри доступной, но обычно является публично доступной
- Работает под управлением IIS7
- Обычно является сайтом ASP.NET

Полнофункциональный IIS – описание

- Web-роль по умолчанию использует полнофункциональный IIS
- Одна Web-роль может содержать множество Web-сайтов под одним публичным IP-адресом
- Могут быть смоделированы приложения, виртуальные директории и привязки
- Все остальное можно реализовать с помощью скриптов (используя администраторский доступ при необходимости)

Сценарий IIS

Фаза	Ключевые стадии
Локальная разработка	• Программирование и развертывание проекта в эмулятор вычислений • Редактирование локальных файлов без дополнительного развертывания в эмулятор

Первичное развертывание (~10 мин.)	• Развертывание сервиса в Windows Azure
	• Определение настроек сервиса Windows Azure (csdef/cscfg) для Web-роли:
	  • Включение удаленного WMSVC, WebDeploy, Powershell, etc.
	  • Конфигурация роли с одним экземпляром.

Итерационная разработка (секунды)	• Программирование в одном проекте Visual Studio • Публикация изменений (например, с помощью Web Deploy)
Развертывание финальной версии(~10 мин.)	• Развертывание сервиса в Windows Azure • *Прим.: если сервис имеет много экземпляров, может быть использован Remote Desktop, но другие средства удаленного управления будут автоматически распределяться по различным экземплярам. Для обхода этого можно использовать эти средства внутри сессии Remote Desktop*

Что такое Worker-роль?

- .NET 3.5 sp1 / 4.0
- «Фоновое» выполнение и выполнение не-HTTP сервиса
- По умолчанию не разрешены входящие подключения

Модель программирования

- Наследуется от RoleEntryPoint
- Метод OnStart()
  - Вызывается Fabric при запуске, позволяет выполнять задачи инициализации.
  - Возвращает балансировщику нагрузки статус «Занят» до того момента, пока не возвратит True.
- Метод Run()
  - Содержит основную логику, обычно бесконечный цикл. Выполнение не должно заканчиваться.
- Метод OnStop()
  - Вызывается при безопасном выключении роли.
  - За 30 секунд можно «прибраться» за ролью.

Сценарии использования

- Опрос очереди
  - Опрос и забор сообщений в цикле while(true)
  - Например, Map/Reduce, «фоновая» обработка изображений
- «Слушатель»
  - Создание TcpListener или WCF Service Host
- Выполнение внешнего процесса
  - Методы OnStart или Run вызывают Process.Start()
  - Задача устанавливает или выполняет «фоновый» /высокоприоритетный процесс
  - Например, запуск сервера баз данных, веб-сервера, распределенного кэша

Что такое VM-роль?

- Разработчик имеет полный контроль над образом ОС
- Возможность развертывания собственных образов WS08R2 Enterprise
- Операторы могут перезагружать, управлять образом и осуществлять управление с помощью Remote Desktop
- Преимущества автоматического управления сервисами, включая улучшения сервисной модели (описанные на следующих слайдах)

Жизненный цикл VM-роли

Сборка образа ВМ	· Конвертация DVD продукта в VHD либо использование готового VHD · Подготовка VHD
Создание сервиса	· Создание сервисной модели на базе подготовленного образа
Публикация образа	· Публикация VHD в блоб в Windows Azure
Развертывание сервиса	· Включая сервисную модель с указанным числом экземпляров. · Сервис упаковывается и загружается как cspkg.
Управление сервисом	· Remote Desktop · Перезагрузка/Развертывание
Обновление сервиса	· Повтор предыдущих шагов с новым образом ОС.

Жизненный цикл VM-роли

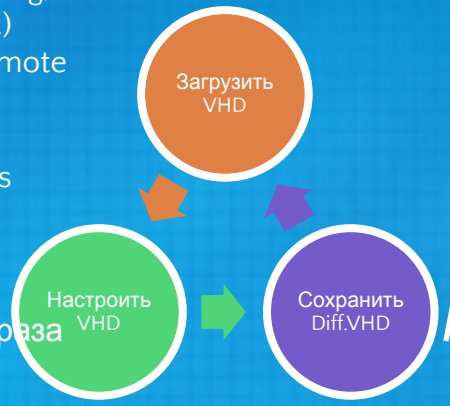
Идентичное/похожее развертывание экземпляров используя загруженные образа ОС (base.VHD + diff.VHD)

Base.VHD

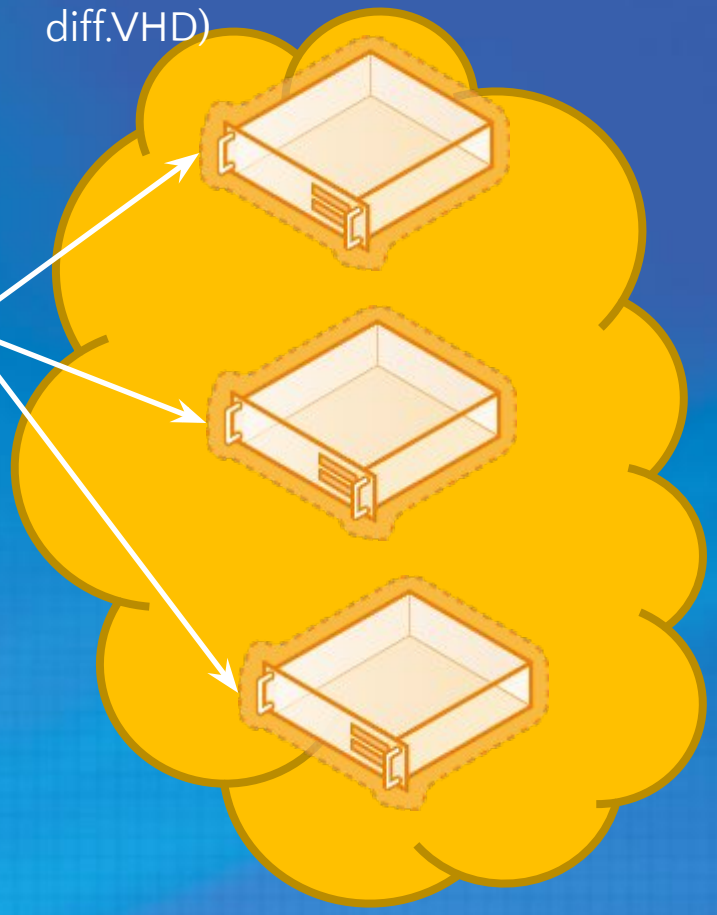
Windows Server 2008 R2 Enterprise

& Дополнительное ПО & Компоненты интеграции Windows Azure
- Агент
- Интерфейс среды выполнения (topo, config, shutdown notification, …)
- Конфигуратор Remote Desktop
- Диагностика
- Драйвер Windows Azure Drives
- Windows Azure Connect

& Генерализация образа (рекомендуемо)



Хранилище блобов



Локально

«Облако»

VM-роль – частые вопросы

- Любое приложение WS08 R2 заработает?
  - Нет, VM-роль унаследовала некоторые ограничения Web/Worker-ролей:
    - По SLA нужно как минимум два идентичных/похожих экземпляра роли
    - Состояние ОС в образе может быть потеряно в случае ошибки оборудования
    - Один публичный IP на сервис (если не использовать Windows Azure Virtual Network)
- Windows Azure позаботится обо *всём*?
  - Нет
    - Клиент сам создаёт и администрирует ВМ
    - Windows Azure не может автоматически распознавать «здоровье» приложений в вашей ВМ
  - Но, если развертывать вместо отдельных ВМ сервис, Windows Azure автоматизирует многие задачи по управлению.

VM-роль – частые вопросы

- Как формируется цена?
  - Аналогично Web/Worker-ролям. Клиент платит почасово в зависимости от размера экземпляра.
- Как работает «облачное» лицензирование?
  - Windows:
    - Лицензия включена в стоимость CPU-часа
    - Статус лицензии образа в расчёт не берётся
  - Приложения: согласно правилам лицензирования приложений

Экземпляры

- Экземпляр – физическая реализация шаблона вашей роли
- Есть несколько размеров экземпляров, но в одной роли экземпляры должны быть одного размера.
- Нельзя менять размер экземпляра во время выполнения

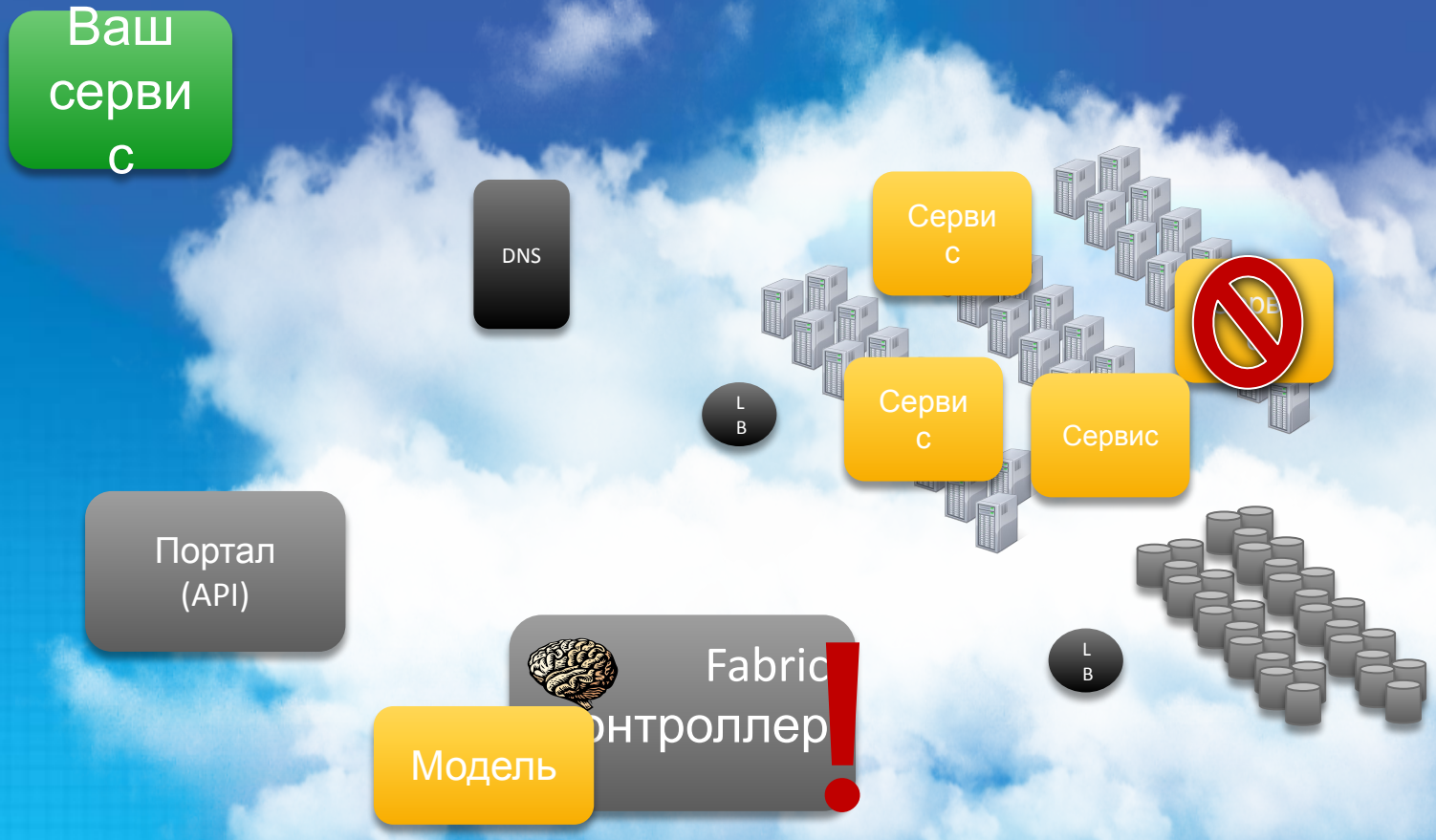
Размер	Количество ядер	Скорость CPU	Память	Стоимость/час
Extra Small	Делится	1.0 GHz	768 MB	$0.05
Small	1	1.6 GHz	1.75 GB	$0.12
Medium	2	1.6 GHz	3.5 GB	$0.24
Large	4	1.6 GHz	7 GB	$0.48
Extra Large	8	1.6 GHz	14 GB	$0.96

Windows Azure

Развертывание сервиса

Масштабирование сервиса

Мониторинг/восстановление



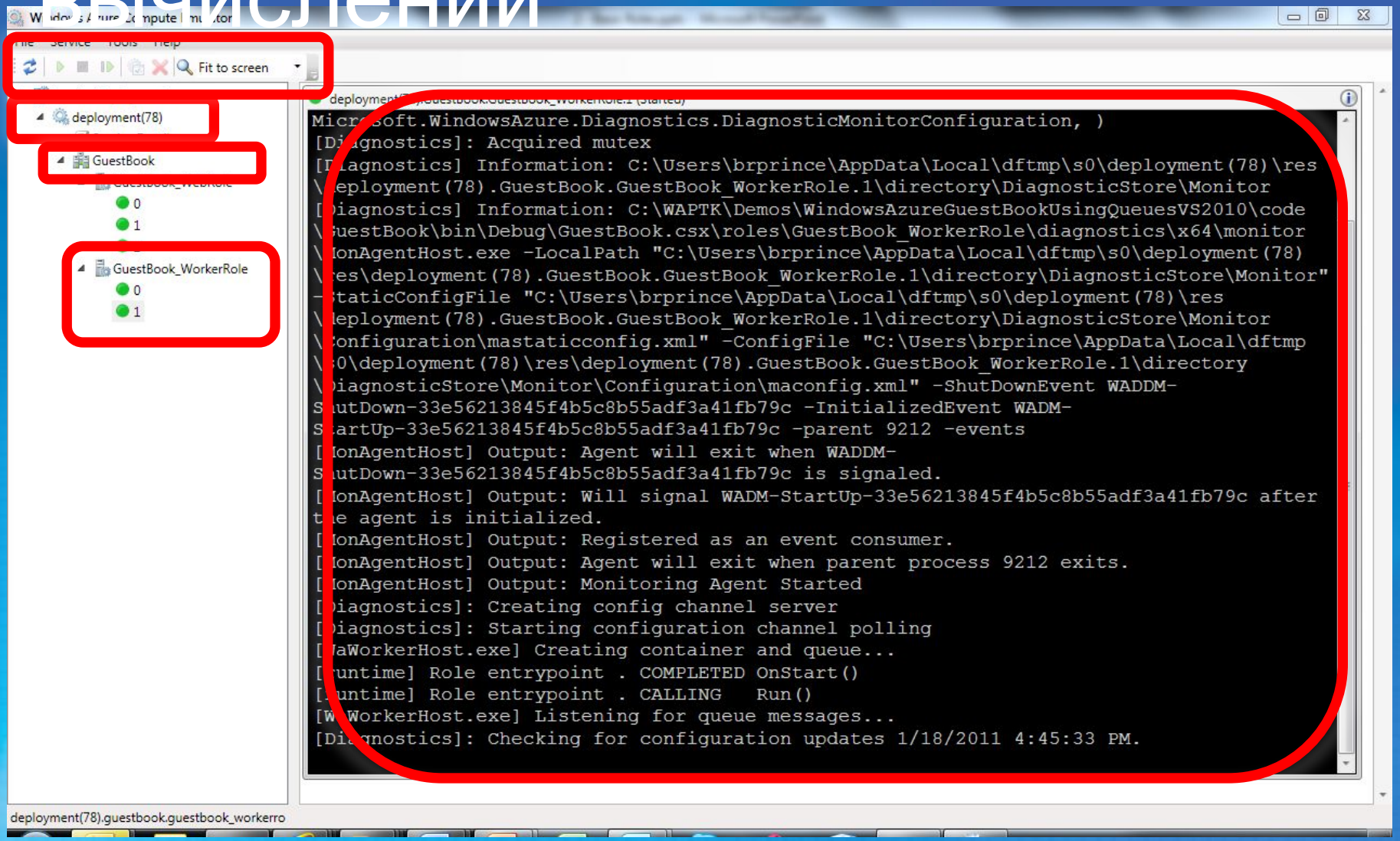
Локальный эмулятор

SDK включает в себя локальную эмуляцию реальных fabric и fabric-контроллера.

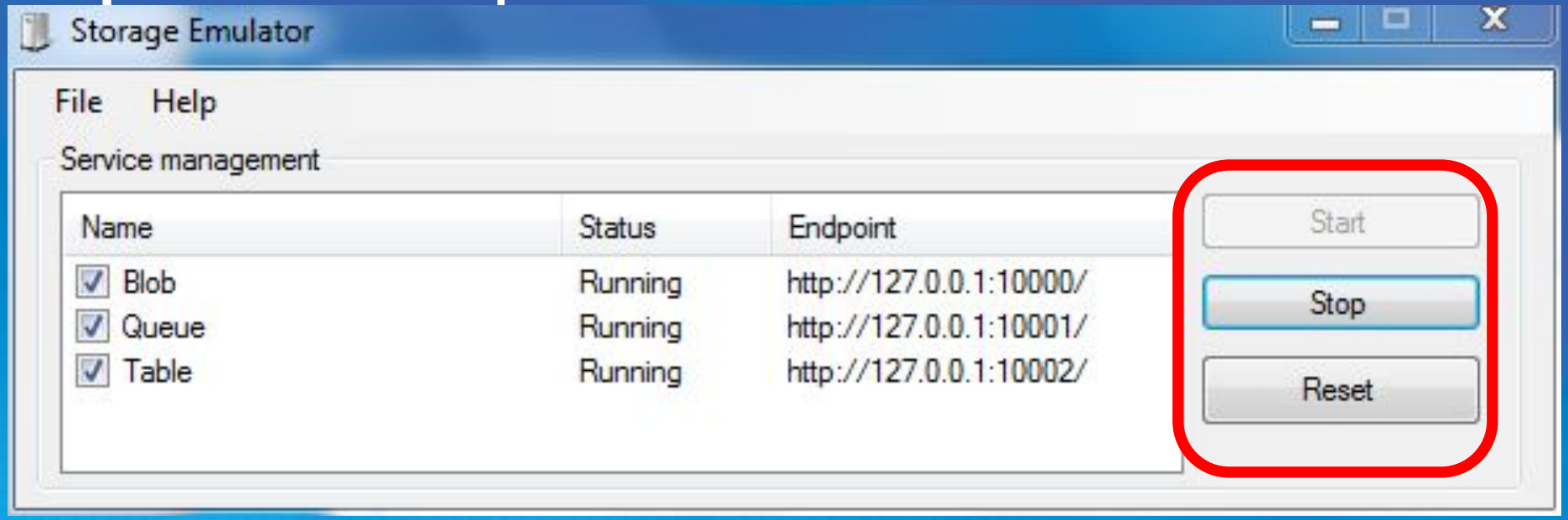
- Основана на 90% кода реального fabric
- Использует локальный экземпляр SQL для эмуляции хранилища
- Лучший способ для отладки вашего приложения
- Позволяет наблюдать за процессами из интерфейса эмулятора вычислений

Иконка эмулятора SDK

Интерфейс эмулятора вычислений



Интерфейс эмулятора хранилища



SQL Express?

- При установленном SQL Express эмулятор хранилища автоматически настроится для его использования при первом запуске
- Если необходимо использовать другой экземпляр SQL:
  - DSInit /sqlInstance:.

Работаем ли мы в Fabric?

```
using Microsoft.WindowsAzure.ServiceRuntime;

namespace HelloCloud
{
    public partial class _Default : System.Web.UI.Page
    {
        protected void Page_Load(object sender, EventArgs e)
        {
            if (RoleEnvironment.IsAvailable == true)
                Literal1.Text = "I am in the fabric.";
            else
                Literal1.Text = "I am running outside of the fabric.";
        }
    }
}
```

Отладка в «облаке»?

Нет. Нет отладки.

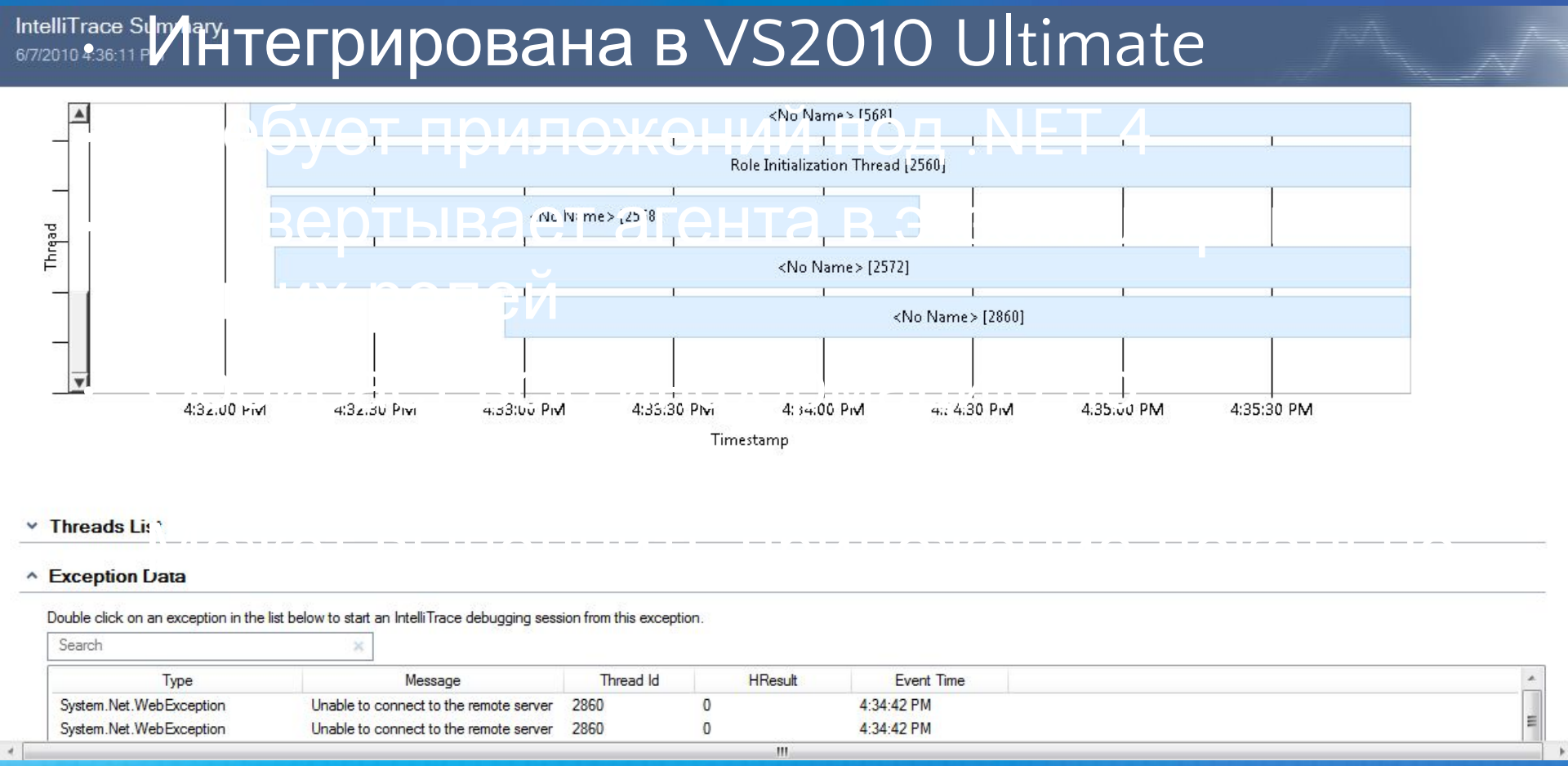
Локальная отладка

- Вы можете отлаживать приложения локально как обычное приложение ASP.NET.
- Полная поддержка нескольких экземпляров

```
protected void Page_Load(object sender, EventArgs e)
{
    if (RoleEnvironment.IsAvailable == true)
        Literal1.Text = "I am in the fabric.";
    else
        Literal1.Text = "I am running outside of the fa
```

Поддержка IntelliTrace

- IntelliTrace поддерживается в Windows
- Интегрирована в VS2010 Ultimate

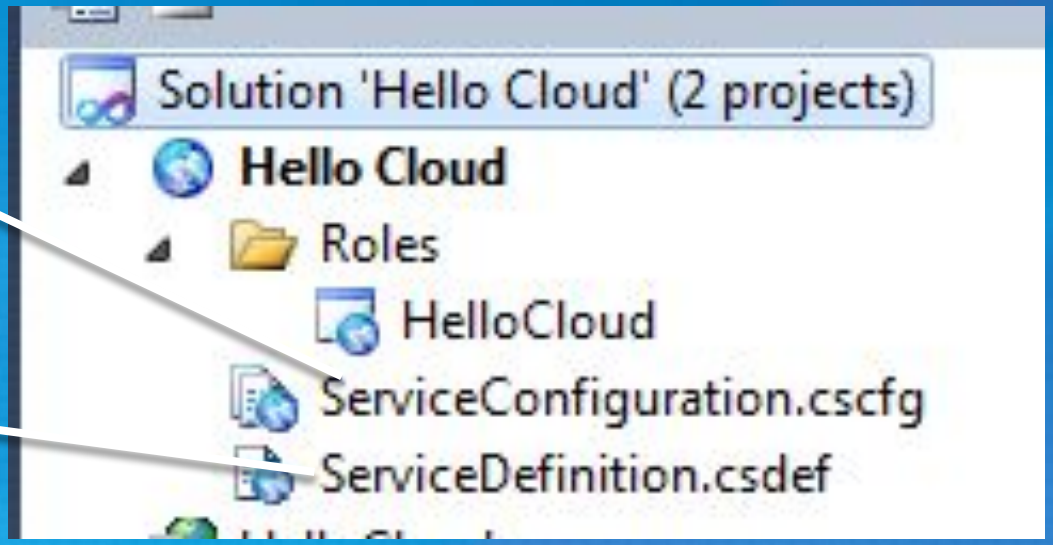


Конфигурация.

- Конфигурация обеспечивается двумя файлами.
  - ServiceDefinition.csdef
  - ServiceConfiguration.cscfg

Конфигурация роли

Конфигурация сервиса



Определение сервиса

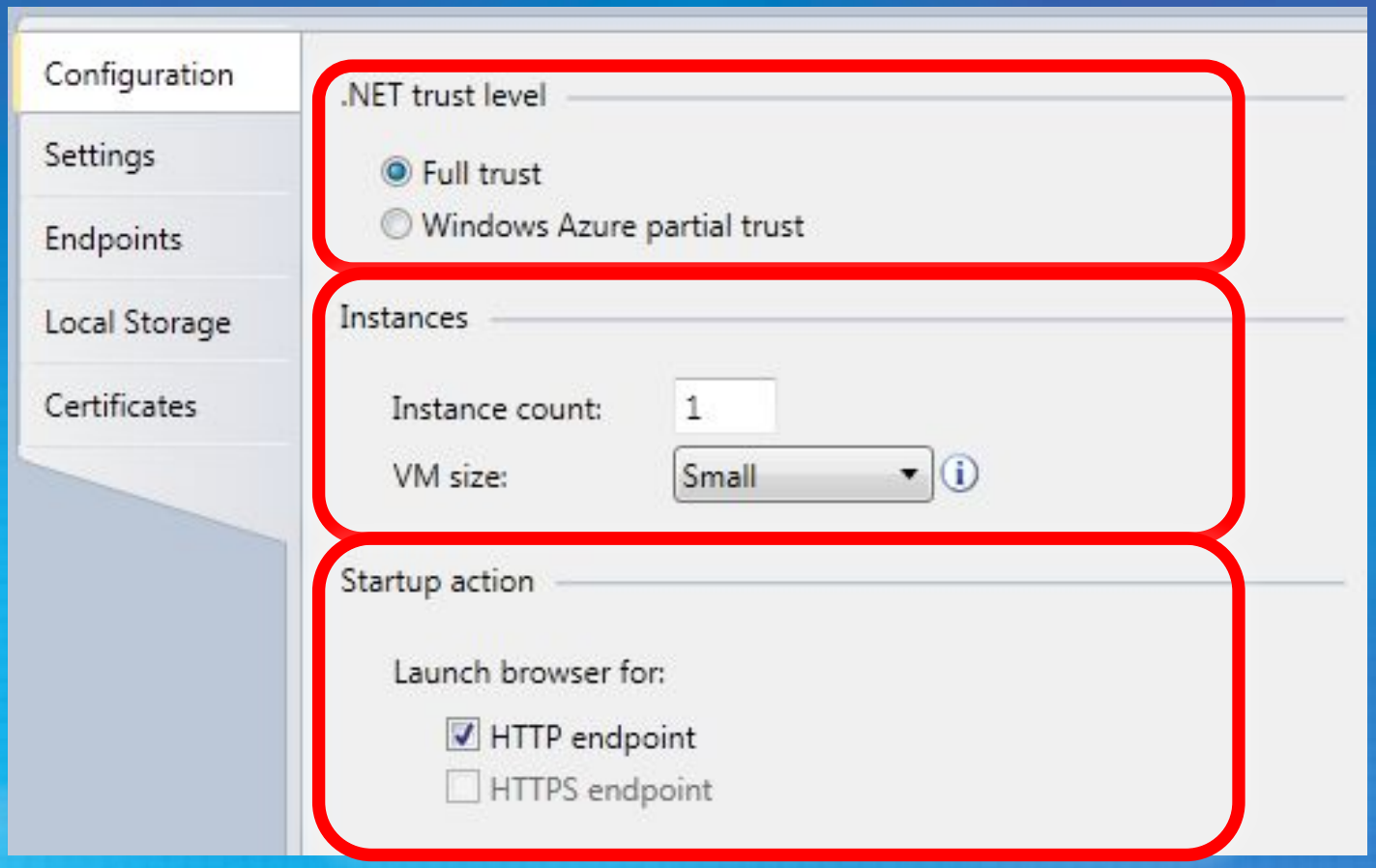
```
<ServiceDefinition name="GuestBook" xmlns="http://schemas.microsoft.com/ServiceHostin
  <WebRole name="GuestBook_WebRole">
    <Sites>
      <Site name="Web">
        <Bindings>
          <Binding name="HttpIn" endpointName="HttpIn" />
        </Bindings>
      </Site>
    </Sites>
    <ConfigurationSettings>
      <Setting name="Microsoft.WindowsAzure.Plugins.Diagnostics.ConnectionString" />
      <Setting name="DataConnectionString" />
    </ConfigurationSettings>
    <Endpoints>
      <InputEndpoint name="HttpIn" protocol="http" port="80" />
    </Endpoints>
  </WebRole>
  <WorkerRole name="GuestBook_WorkerRole">
    <ConfigurationSettings>
      <Setting name="Microsoft.WindowsAzure.Plugins.Diagnostics.ConnectionString" />
      <Setting name="DataConnectionString" />
    </ConfigurationSettings>
  </WorkerRole>
</ServiceDefinition>
```

Конфигурация сервиса

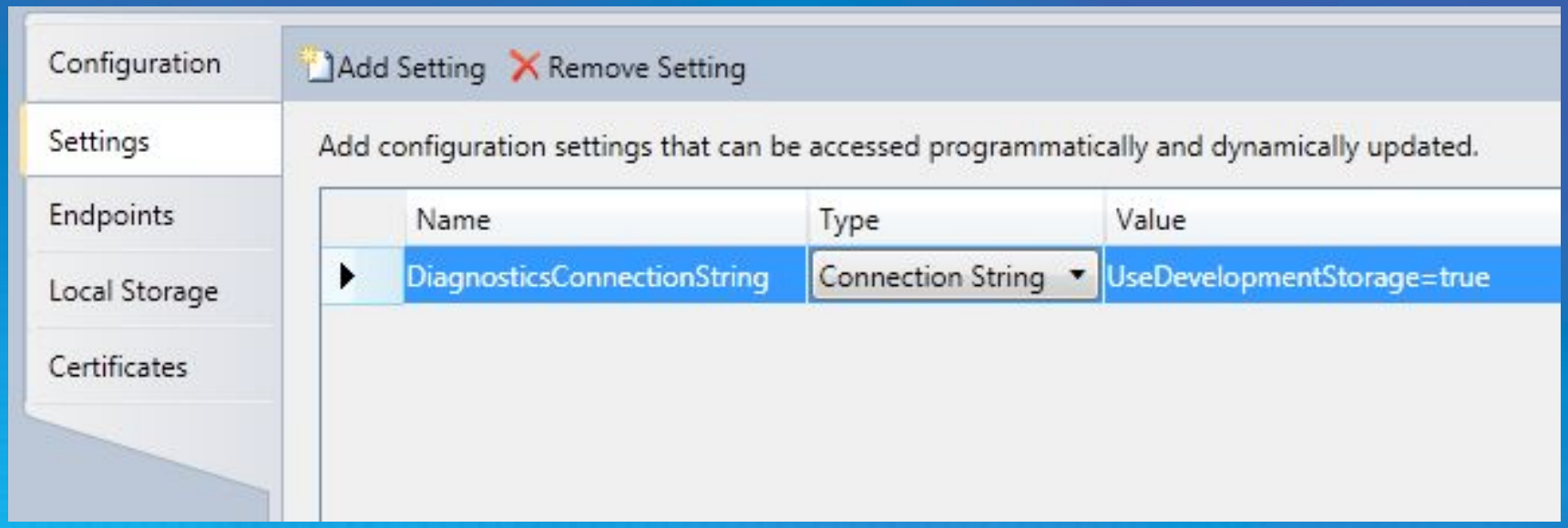
```
<ServiceConfiguration serviceName="GuestBook" xmlns="http://schemas.microsoft.com/
  <Role name="GuestBook_WebRole">
    <Instances count="1" />
    <ConfigurationSettings>
      <Setting name="DataConnectionString"
               value="UseDevelopmentStorage=true" />
      <Setting name="Microsoft.WindowsAzure.Plugins.Diagnostics.ConnectionString"
               value="UseDevelopmentStorage=true" />
    </ConfigurationSettings>
  </Role>
  <Role name="GuestBook_WorkerRole">
    <Instances count="1" />
    <ConfigurationSettings>
      <Setting name="DataConnectionString"
               value="UseDevelopmentStorage=true" />
      <Setting name="Microsoft.WindowsAzure.Plugins.Diagnostics.ConnectionString"
               value="UseDevelopmentStorage=true" />
    </ConfigurationSettings>
  </Role>
</ServiceConfiguration>
```

GUI

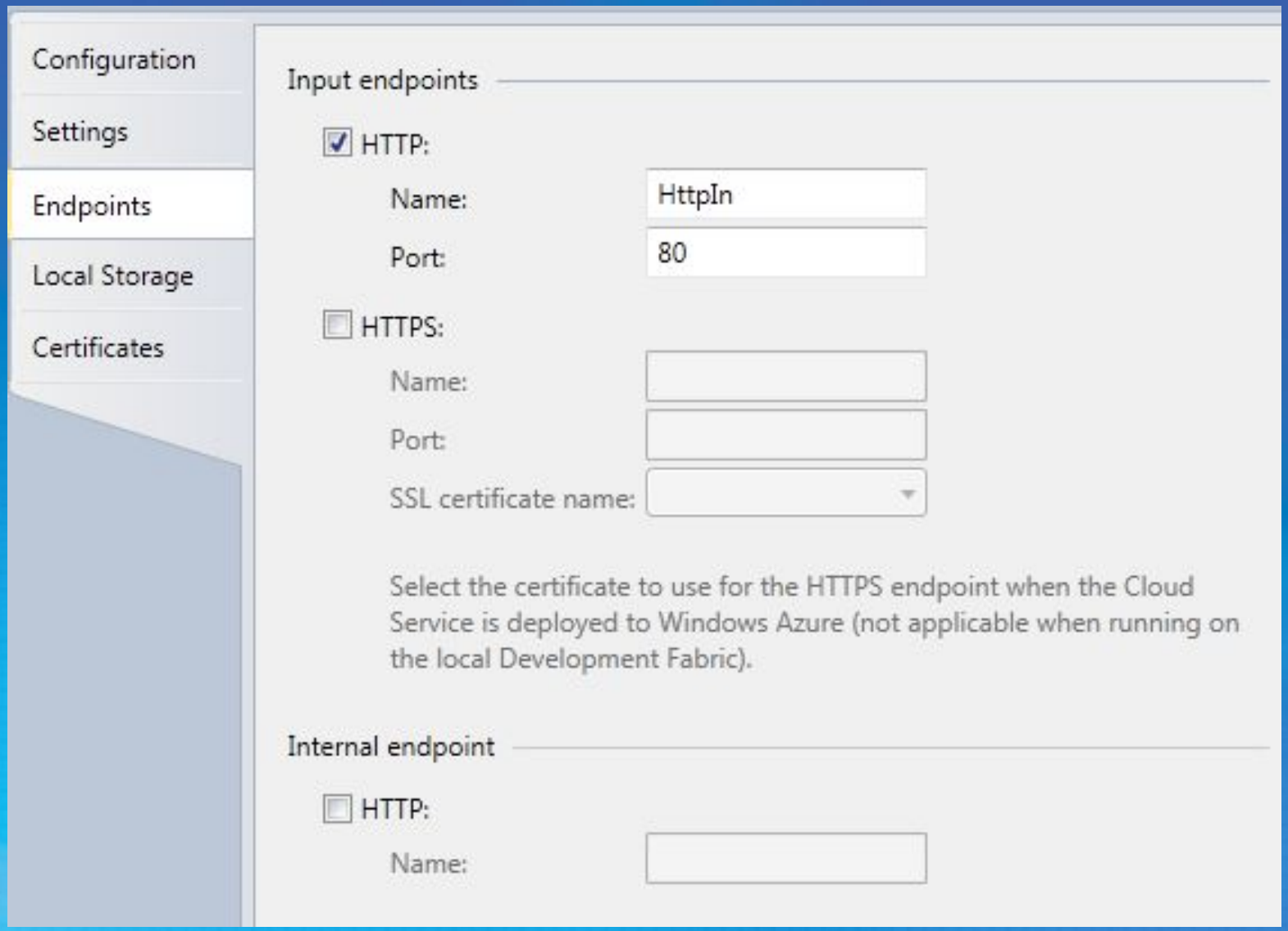
Нажмите два раза на имени роли в проекте



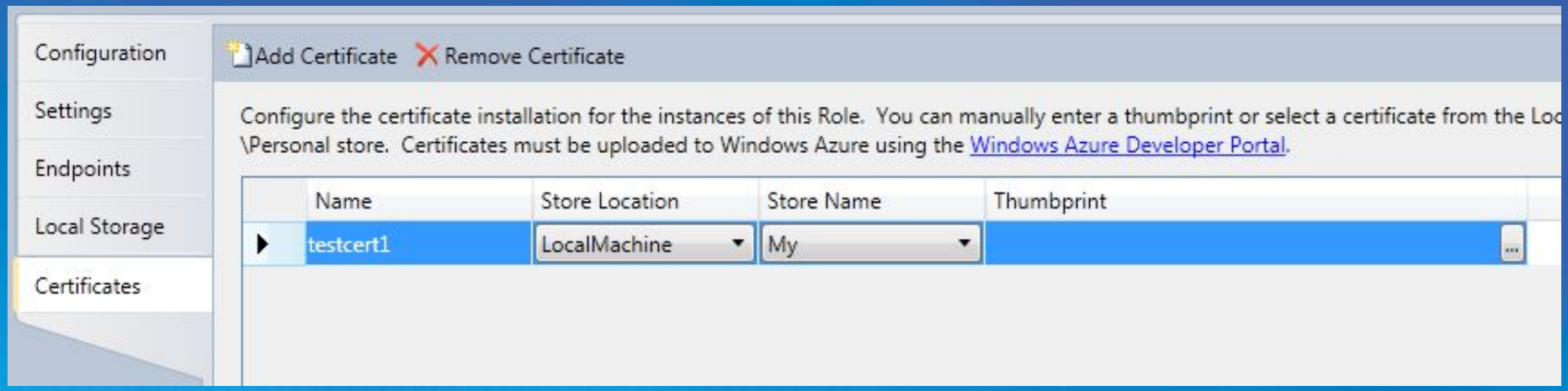
Настройки


Configuration
Settings
Endpoints
Local Storage
Certificates
Add Setting
Remove Setting
Add configuration settings that can be accessed programmatically and dynamically updated.
Name
Type
Value
DiagnosticsConnectionString
Connection String
UseDevelopmentStorage=true

Точки входа


Configuration
Settings
Endpoints
Local Storage
Certificates
Input endpoints
HTTP:
Name:
HttpIn
Port:
80
HTTPS:
Name:
Port:
SSL certificate name:
Select the certificate to use for the HTTPS endpoint when the Cloud Service is deployed to Windows Azure (not applicable when running on the local Development Fabric).
Internal endpoint
HTTP:
Name:

Сертификаты



Hello Cloud

демонстрация

Три варианта при развертывании сервиса

- Visual Studio
- Портал
- API

Развертывание в «облако»

- Вы должны создать аккаунт в Azure, сервис и развернуть сервис.
- VS собирает два файла
  - Зашифрованный пакет с кодом
  - Конфигурационный файл
- Может занимать 20 минут
- В случае разработки вы можете использовать Web Deploy

Портал

Windows Azure

New Hosted Service

New Produ Deploym

New

Deployment Heal

Affinity Groups

Management Cer

Hosted Services

Storage Accounts

User Managemer

VM Images

Configure OS

Create a new Hosted Service

Choose a subscription

Field: brprince

Enter a name for your service

Wicked Syrup Commerce

Enter a URL prefix for your service

wickedsyrup cloudapp.net

Choose a region or affinity group

Southeast Asia | Create or choose an affinity group

Deployment options

- Deploy to stage environment
- Deploy to production environment
- Do not deploy

☑ Start after successful deployment

Deployment name

v1 QA test

Package location

Browse Locally... | Browse Storage...

Configuration file

Browse Locally... | Browse Storage...

Add Certificate

OK | Cancel

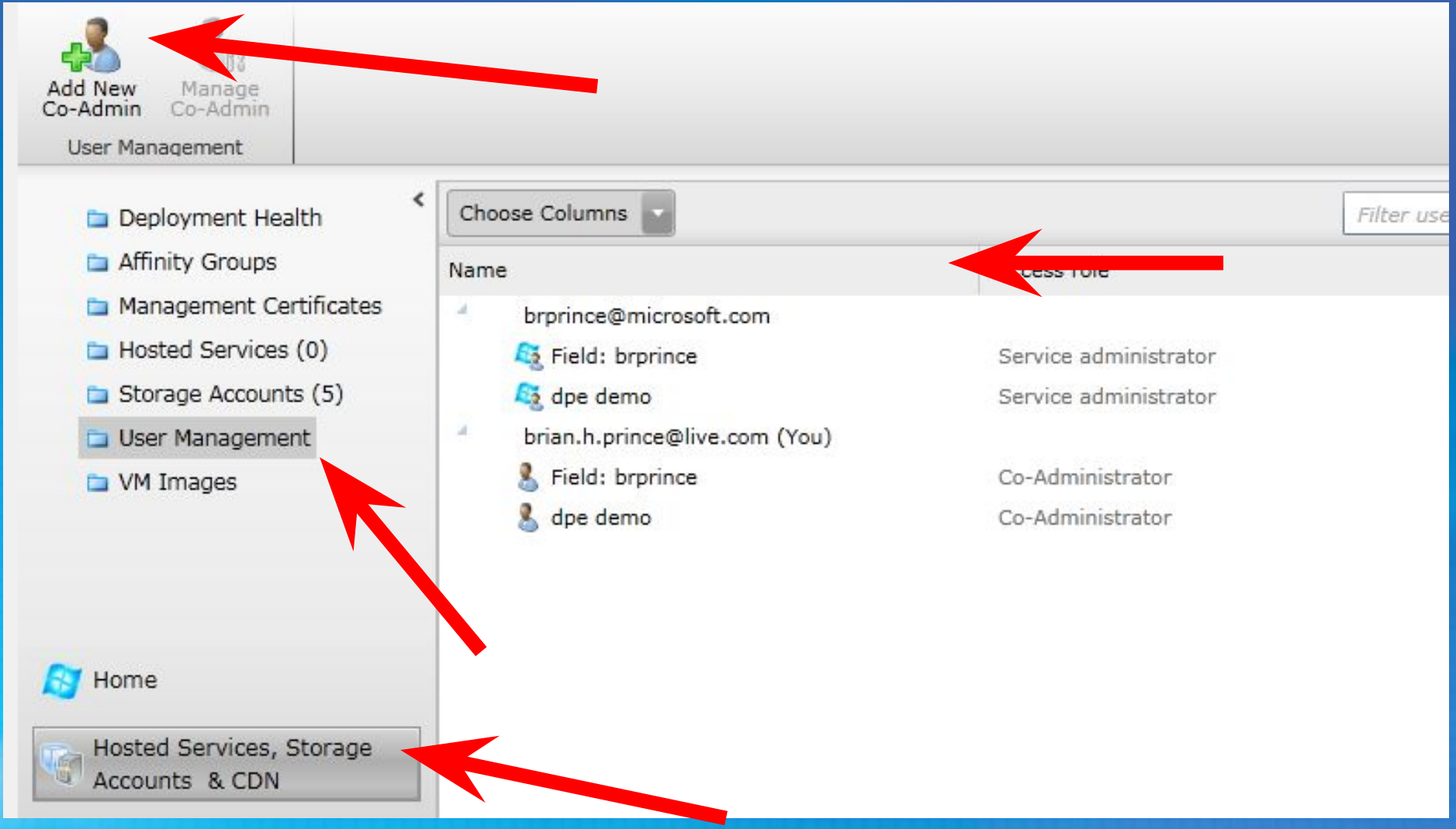
Развертывание в «облако»

демонстрация

DNS

- Все сервисы получают адрес вида *.cloudapp.net
  - myservicename.cloudapp.net
  - TTL записи – 10 секунд
- Обычный подход – создавать CNAME на *.cloudapp.net
  - Нужно два DNS lookup
  - Ограниченное кэширование (из-за малого TTL)
- Нет официальной поддержки записей типа A
- IP развертывания фиксируется на время жизни

Портал – администраторы



Q & A

соображения?

Hello Windows Azure

- Получите аккаунты Azure.
- Выполните демонстрацию “Hello Windows Azure VS2010”.

Время на лабораторную