CITRIX

App Orchestration 2.0

App Orchestration Isolation

Prepared by: Robert Hyde

Version: 1.0

Last Updated: December 11, 2013

Contents

Overview 3
Delivery isolation 3
Shared Delivery Groups 3
Private Delivery Groups 4
Private Delivery Sites 5
Tenant StoreFront isolation 5
Shared sites 6
Private sites 6
Private server groups 7
Networks required for isolation 8
Required networks 8
Optional networks 8

Overview

In all networks, you need the ability to isolate certain parts, be it an isolated XenDesktop site for your payroll division or a separate Session Machine for a tenant to run specific licensed software. App Orchestration accommodates this need for isolation.

This document provides an introduction to network isolation within App Orchestration, discusses how network isolation works, and then describes the networks that need to be created in each case.

Within App Orchestration there are two areas where you can specify the levels of isolation, delivery isolation and tenant StoreFront isolation.

Delivery isolation

When creating an offering, you must specify the level of isolation for your Session Machines and Delivery Sites. Three isolation levels are available.

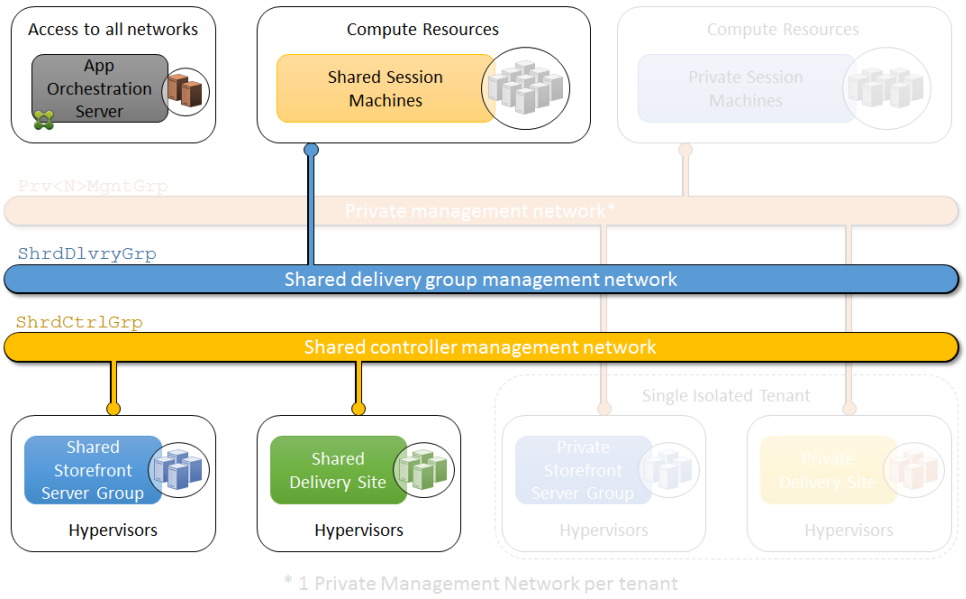
- Shared Delivery Group—both Session Machines and the Delivery Site are shared with other tenants.
- Private Delivery Group—Session Machines are private, but the Delivery Site is shared.
- Private Delivery Site—both Session Machines and the Delivery Site are private, and are not available to other tenants.

The following table compares the characteristics of the delivery isolation levels.

Isolation Level	Session Machines and Delivery Sites	Session Machine Network	StoreFront Server Group Network
Shared Delivery Group	Shared Session Machines Shared Delivery Site	Shared Delivery Group network	Shared Delivery Controller management network
Private Delivery Group	Private Session Machines Private Delivery Site	Private management network (dedicated to a specific tenant) or shared Delivery Group network (if tenant has no private management network)	Shared Delivery Controller management network
Private Delivery Site	Private Session Machines Private Delivery Site	Private management network (dedicated to a specific tenant) or shared Delivery Group network (if tenant has no private management network)	Private management network (dedicated to a specific tenant)

Shared Delivery Groups

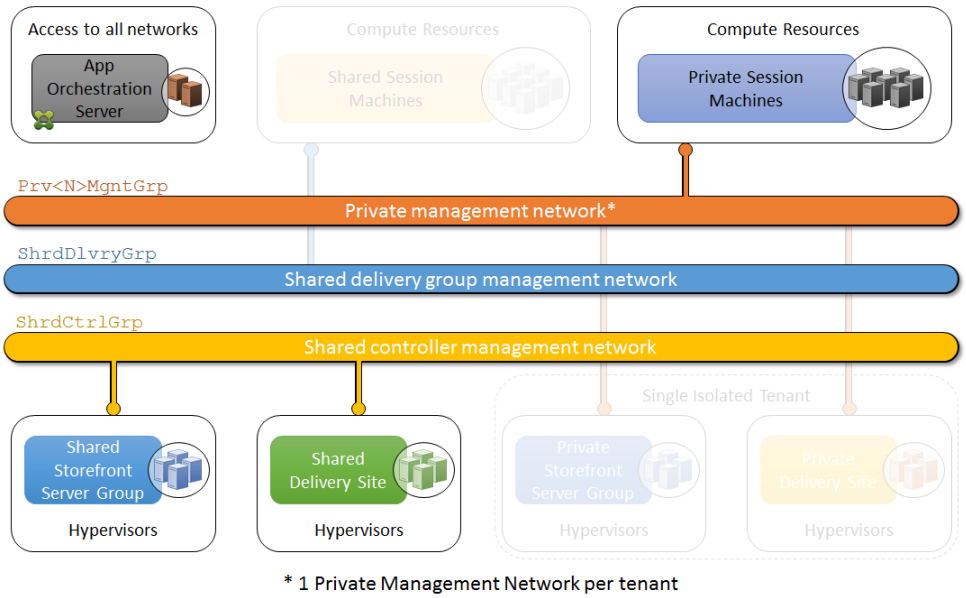
For tenants who do not need any form of isolation within the datacenter, you can use shared Delivery Groups. In these groups, the Session Machines and Delivery Site are connected to the shared Delivery Group network and the shared Delivery Controller management network, respectively. At this isolation level, hosted applications and desktops run on machines that serve the users of multiple tenants, and the same shared Delivery Site brokers the connections for these users.



Shared Delivery Group Isolation Level

Private Delivery Groups

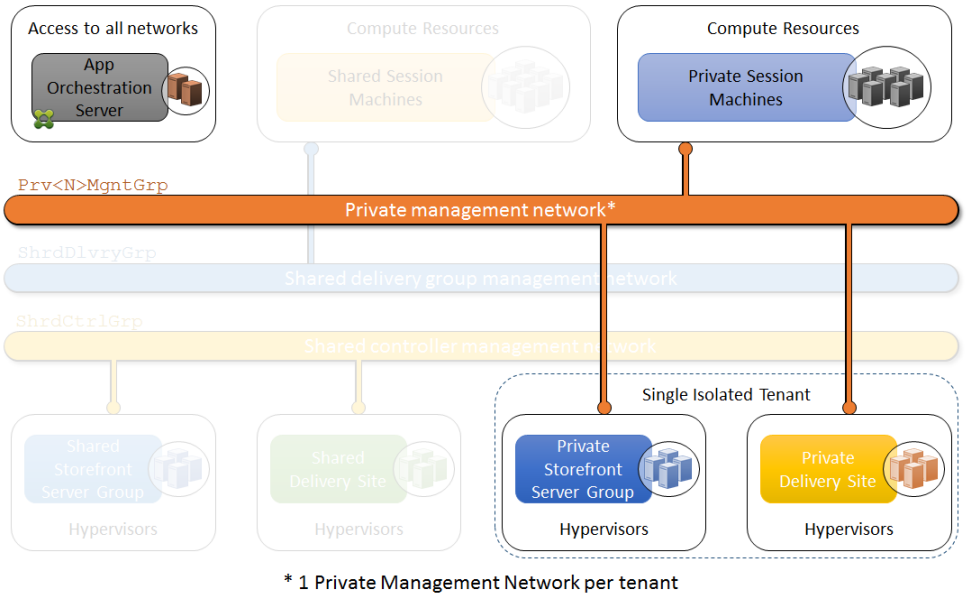
For tenants who require that only Session Machines are isolated within the datacenter, you can configure private Delivery Groups. In these groups, Session Machines and the shared Delivery Site are connected to the tenant's private management network and the shared Delivery Controller management network, respectively. At this isolation level, hosted applications and desktops run on machines that only the tenant's users can access, but their connections are still brokered by the same shared Delivery Site.



Private Delivery Group Isolation Level

Private Delivery Sites

For tenants who need both Session Machines and the Delivery Site isolated within the datacenter, you can offer private sites. In these groups, the Session Machines and Delivery Site are connected to the tenant's private management network. At this isolation level, hosted applications and desktops run on machines that only the tenant's users can access and their connections are brokered by a Delivery Site that is dedicated exclusively to the tenant.



Private Site Isolation Level

Tenant StoreFront isolation

When delivering offerings to tenant users, you specify the level of StoreFront isolation for each tenant you import into App Orchestration. Three types of isolation are available.

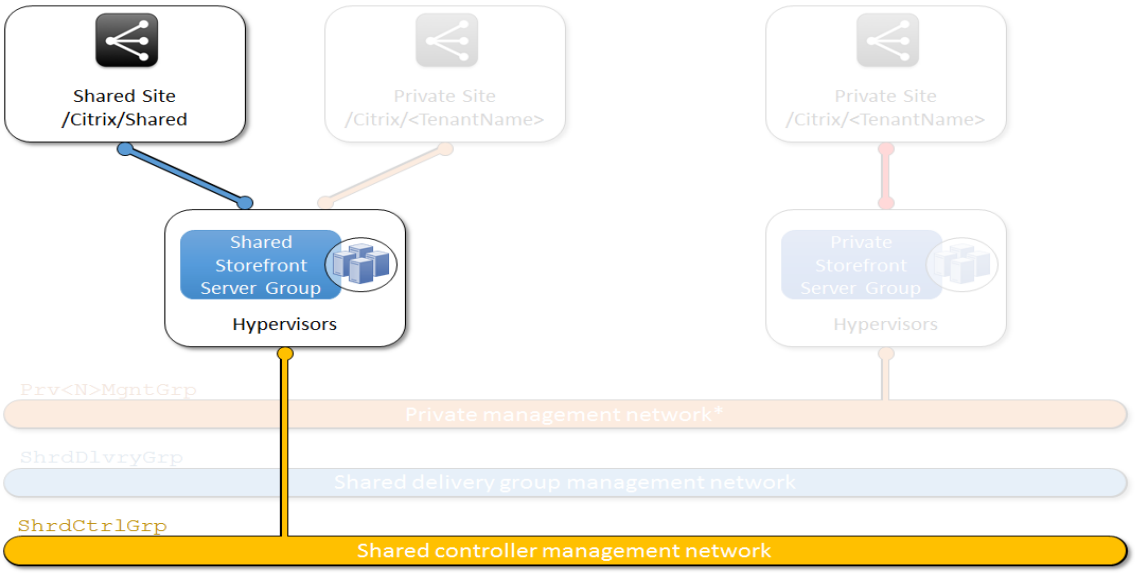
- Shared site—the StoreFront server group is shared between tenants and they use a shared store.
- Private site—the StoreFront server group is shared, but the tenants each have their own store.
- Private server group—the StoreFront server group is dedicated to a specific tenant and provides a store for that tenant only.

The following table compares the characteristics of the StoreFront isolation levels.

Isolation Level	Store	StoreFront Server Group	StoreFront Server Group Network
Shared site	*sharedFQDN*/ Citrix/Shared	Shared	Shared Delivery Controller management network
Private site	*sharedFQDN*/ Citrix/*tenantname*	Shared	Shared Delivery Controller management network
Private server group	*sharedFQDN*/ Citrix/*tenantname*	Private	Shared Delivery Controller management network or private management network (dedicated to a specific tenant)

Shared sites

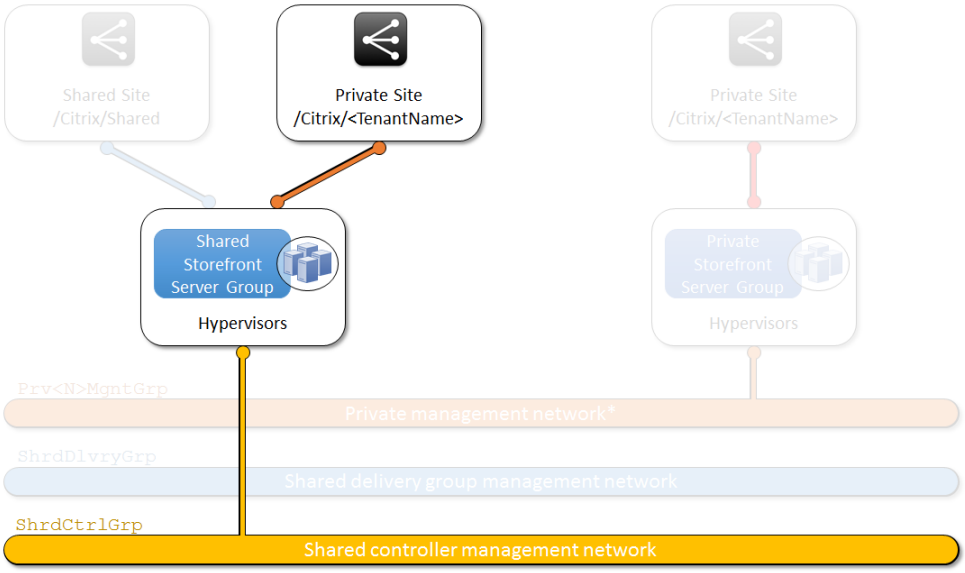
For tenants who do not require any form of StoreFront isolation within the datacenter, you can use shared sites. At this isolation level, users log on to a shared StoreFront store on a shared StoreFront server group. The shared StoreFront server group is connected to the shared Delivery Controller management network. Users of multiple tenants log on to StoreFront using the same URL, which typically takes the form https://*sharedservergroupFQDN*/Citrix/Shared.



Shared Site

Private sites

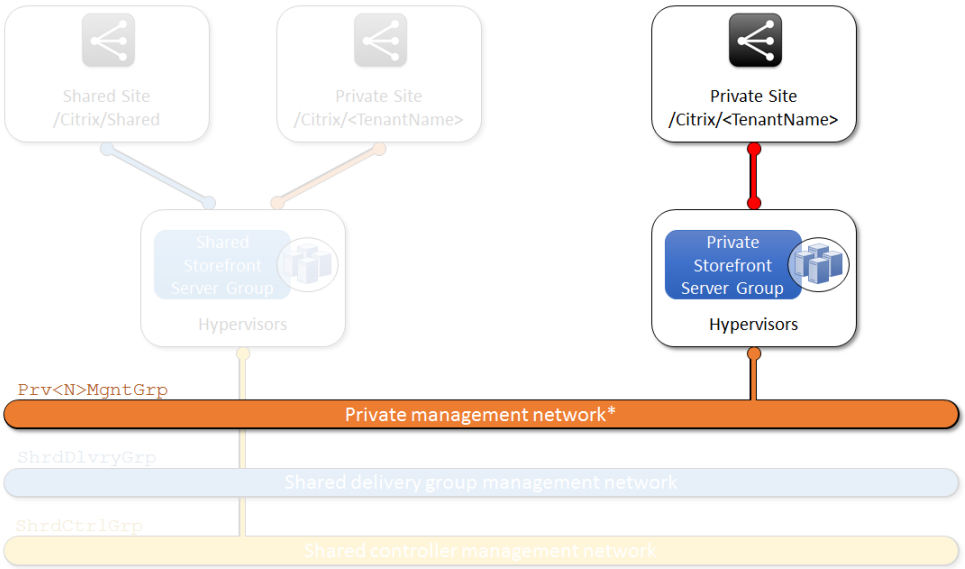
For tenants who require an isolated StoreFront store for their users, you can provide private sites. At this isolation level, a shared StoreFront server group is used to host a private StoreFront store for the tenant. As with the shared site isolation level, the shared StoreFront server group is connected to the shared Delivery Controller management network. The tenant's users log on to a private StoreFront store using a tenant-specific URL, which typically takes the form https://*sharedservergroupFQDN*/Citrix/*tenantname*.



Private Site

Private server groups

For tenants who require a completely isolated StoreFront store and server group, you can offer private server groups. At this isolation level, the private StoreFront server group is either connected to the tenant's own private management network or the shared management network if the tenant does not have an isolated network. The tenant's users log on to StoreFront using a tenant-specific URL that points to a private StoreFront server group on the relevant network. The URL typically takes the form https://*privateservergroupFQDN*/Citrix/*tenantname*.



Private Server Group

Networks required for isolation

In App Orchestration, there are two types of networks.

- Required networks must be included in order for network isolation to work.
- Optional networks can be attached to Session Machines to carry additional traffic as required.

These networks are identified using network labels that are set on every hypervisor running App Orchestration. Note that the network labels that you enter in App Orchestration must match exactly (including the case) the labels on the hypervisors to enable App Orchestration to find the networks. For more information about setting network labels for the hypervisors in your environment, refer to the following documentation.

- XenServer

  "Creating VLANs" in *Citrix XenServer 6.2.0 Administrator's Guide*

  http://docs.vmd.citrix.com/XenServer/6.2.0/1.0/en_gb/reference.html#networking-standalone_host_config-vlans
- Microsoft System Center Virtual Machine Manager

  "Networking in VMM 2012 SP1 - Logical Networks (Parts I–V)" in *VMM 2012 Survival Guide*

  http://social.technet.microsoft.com/wiki/contents/articles/3053.vmm-2012-survival-guide.aspx
- VMware vSphere

  "Add a Virtual Machine Port Group with the vSphere Web Client" in *VMware vSphere 5.5 Documentation Center*

  http://pubs.vmware.com/vsphere-55/topic/com.vmware.vsphere.networking.doc/GUID-004E2D69-1EE8-453E-A287-E9597A80C7DD.html

Required networks

To provide network isolation, you must include the following networks.

- Shared Delivery Controller management network—contains the shared Delivery Site and is defined during initial configuration of App Orchestration.
- Shared Delivery Group network—contains shared Session Machines and is defined during initial configuration of App Orchestration.
- Private management networks—contain private Session Machines and Delivery Sites. Add one for each tenant that is subscribed to an offering with either private Delivery Group or private site isolation.

Optional networks

In addition to the required networks, you can also add shared Delivery Group networks for shared Session Machines and private Delivery Group networks for private Session Machines. These networks are not required for isolation within App Orchestration, but are used to carry any additional traffic that tenants may require for their shared or private Session Machines. Optional networks must be connected as network interface controllers (NICs) to the VM that will be used to create a master image for the Session Machine Catalog.