

Windows Docker简介

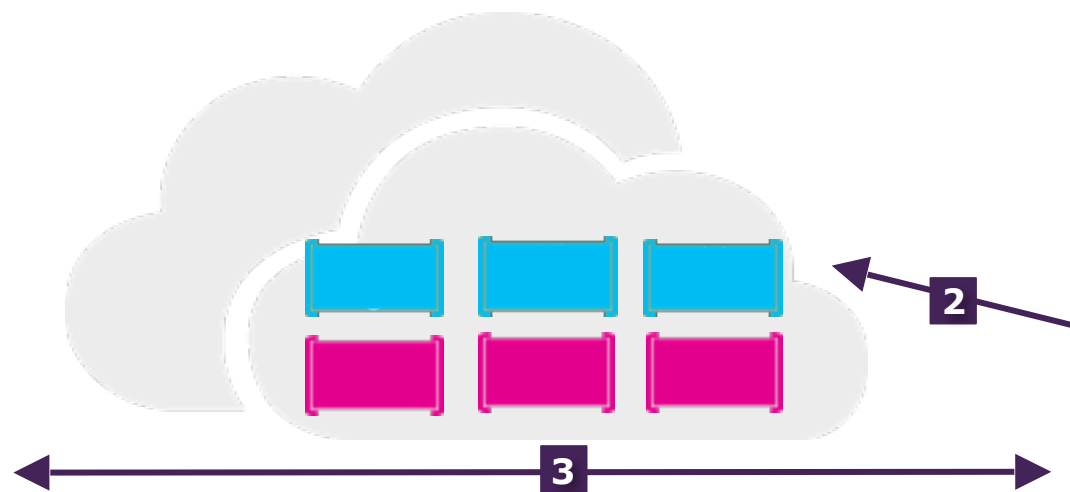
彭爱华

王阳明先生的知行合一， DevOps

开发者 更新, 迭代, 以及部署新版的容器



开发者 在容器中进行开发和测试, 和开发工具环境结合, 如 Visual Studio



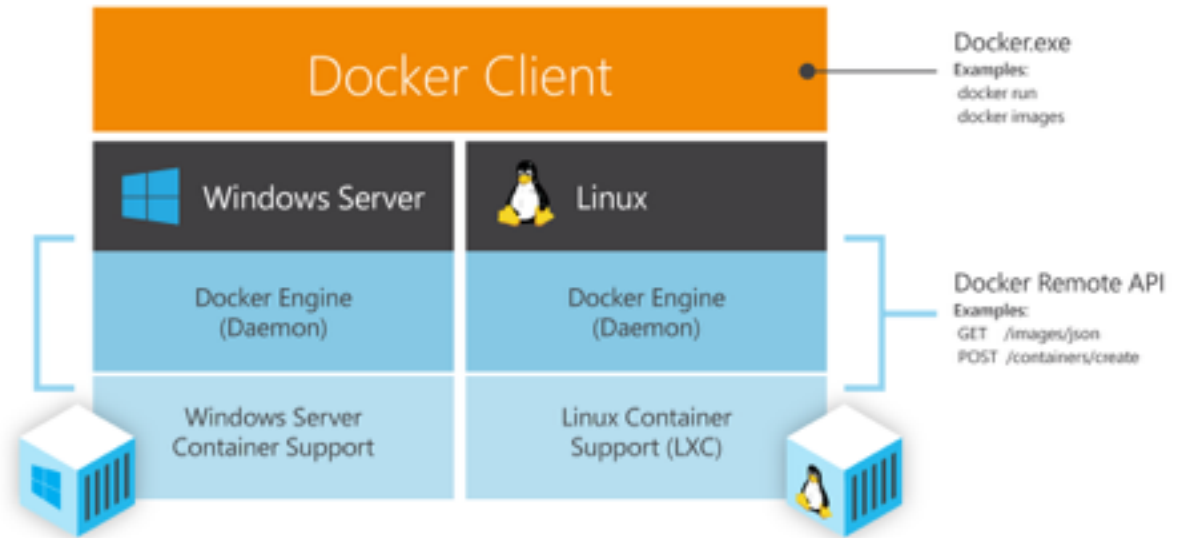
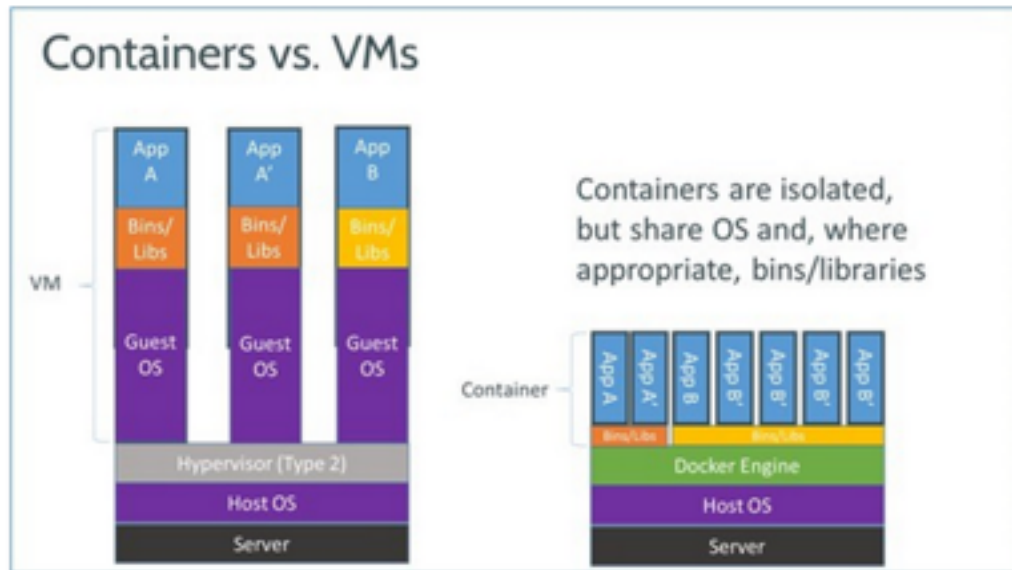
运维人员 和 开发者 协作提供应用计量和深入分析信息



运维人员 从中央库中自动部署应用并对应用进行监控。

何为Windows Containers

- 双胞胎：Windows Server Container 和Hyper-V Container
- 可以用Docker API管理
- 集成到Docker Hub



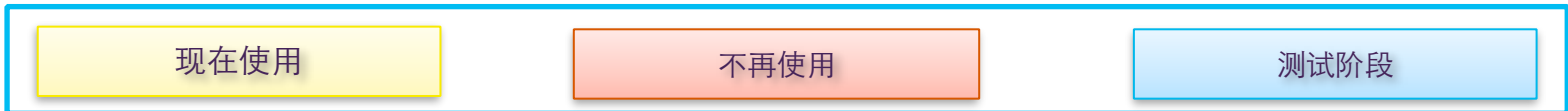
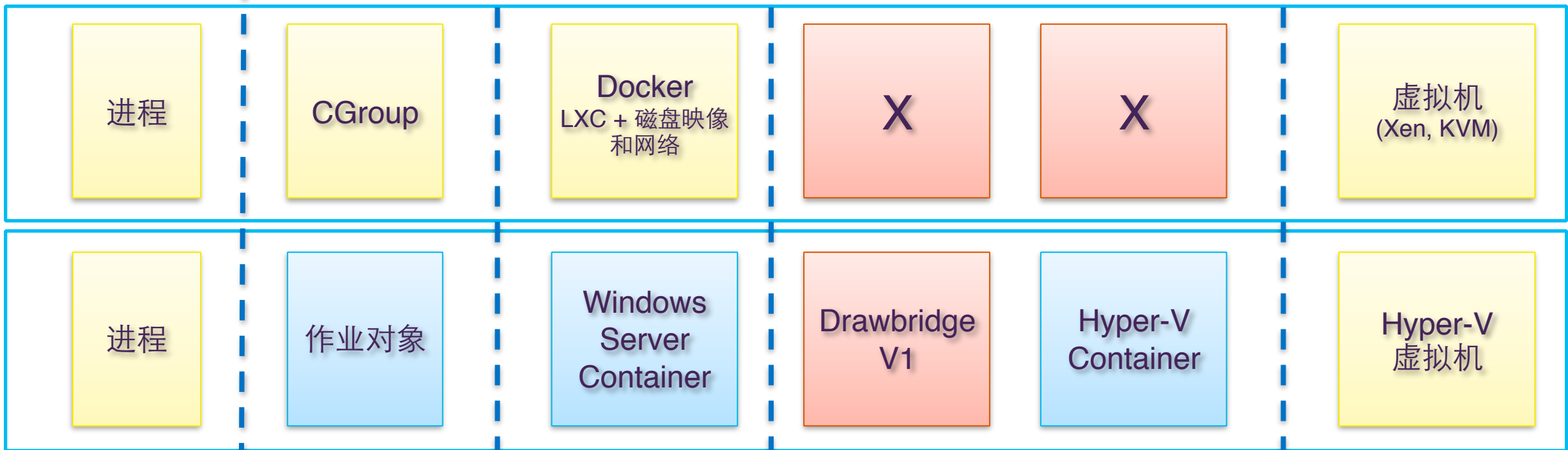
技术沿革图

资源配额
和限制

状态
隔离

多租户安全

硬件虚拟化



技术对比

	Hyper-V Container	Windows Server Container	Docker	虚拟机
多租户安全	是	否	否	是
资源管控	是	是	是	是
并发度	中-高	高	高	低
启动时间	低-中	低	低	高
磁盘占用	低	低	低	高
兼容性	中-高	中-高	中-高?	高

Windows Server Container和Hyper-V Container区别

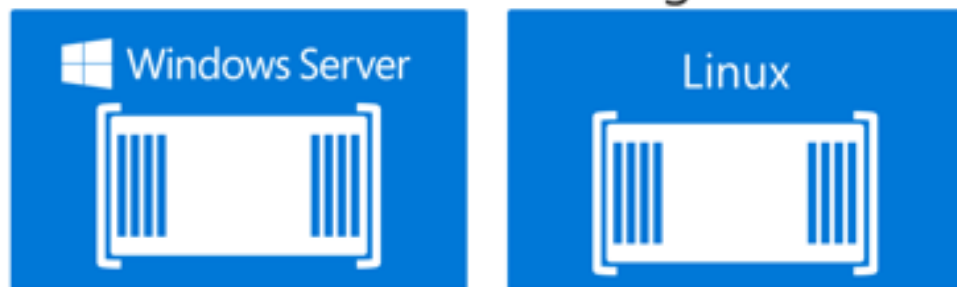
	Windows Server Container	Hyper-V Container
内核	同宿主机	独立内核
容器内管理权限	是	是
系统服务	共享主机上的某些服务	独立新服务
资源管控	统一管控	
映像打包	同样的映像格式	
加域	否	支持
<i>SID</i>	和主机一样	独立

微软容器技术全套工具.

Container Management



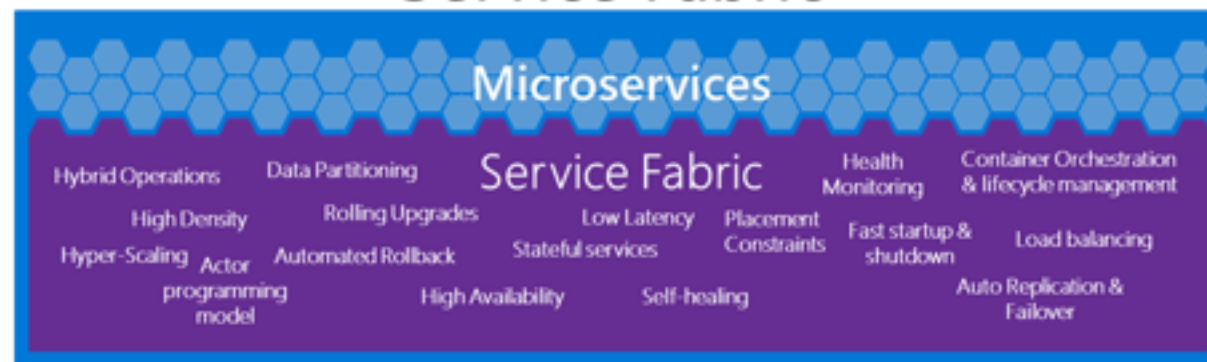
Container Technologies



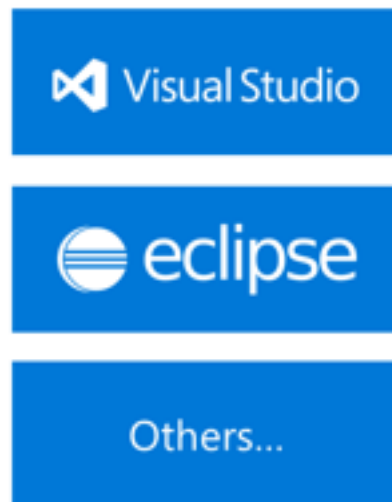
Microsoft Cloud



Service Fabric



Development Environments



Platform Services

Security & Management

- Portal
- Active Directory
- Multi-Factor Authentication
- Automation
- Key Vault
- Store / Marketplace
- VM Image Gallery & VM Depot

Compute

- Cloud Services
- Service Fabric
- Batch
- Remote App

Web and Mobile

- Web Apps
- API Apps
- API Management
- Mobile Apps
- Logic Apps
- Notification Hubs

Developer Services

- Visual Studio
- Azure SDK
- Team Project
- Application Insights

Hybrid Operations

- Azure AD Connect Health
- AD Privileged Identity Management
- Backup
- Operational Insights
- Import/Export
- Site Recovery
- StorSimple

Integration

- Storage Queues
- Biztalk Services
- Hybrid Connections
- Service Bus

Analytics & IoT

- HDInsight
- Machine Learning
- Data Factory
- Event Hubs
- Stream Analytics
- Mobile Engagement

Data

- SQL Database
- SQL Data Warehouse
- Redis Cache
- Search
- DocumentDB
- Tables

Media & CDN

- Media Services
- Content Delivery Network (CDN)

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- BLOB Storage
- Azure Files
- Premium Storage

Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- Application Gateway

Datacenter Infrastructure (24 Regions, 19 Online)



Windows容器和Linux容器，各有多少系统进程？

Container OS：用户模式OS

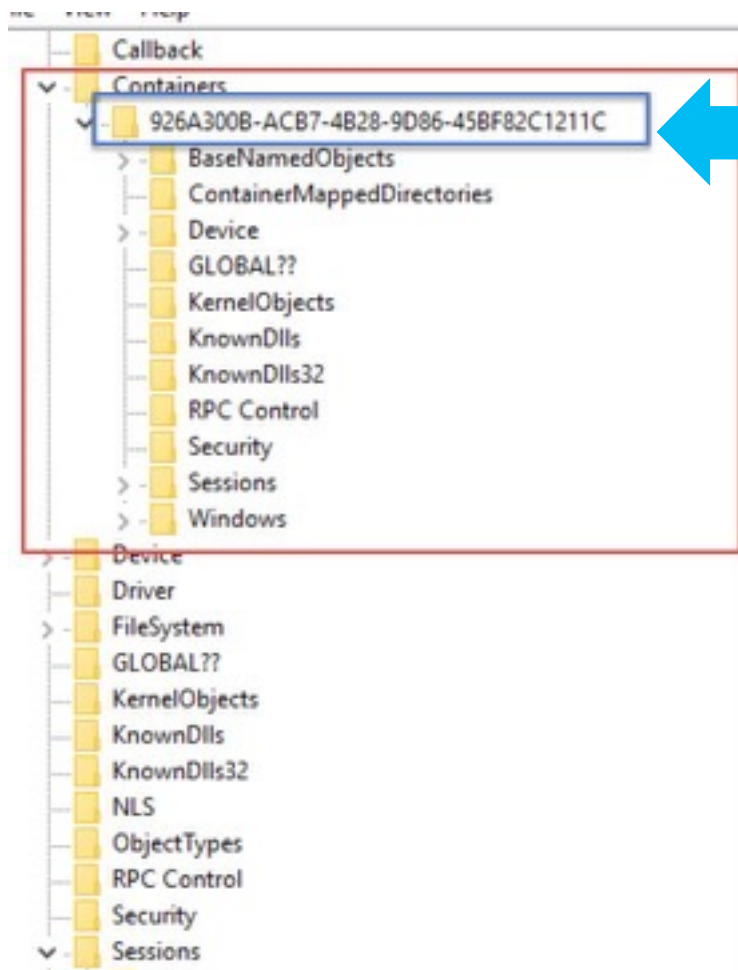
```
mark@linuxdocker:~$ docker run -i -t ubuntu /bin/bash
root@9fd176c080ce:/# ps -aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1   0.9  0.0  18172  3072 ?        Ss   13:21   0:00 /bin/bash
root          15   0.0  0.0   1552   1996 ?        R+   13:22   0:00 ps -aux
```

```
PS C:\Users\Administrator> Enter-Pssession -ContainerName psdemo01 -Runasadmin
[psdemo01]: PS C:\Windows\system32> Get-Service | Where-Object {$_.status -eq "running"}

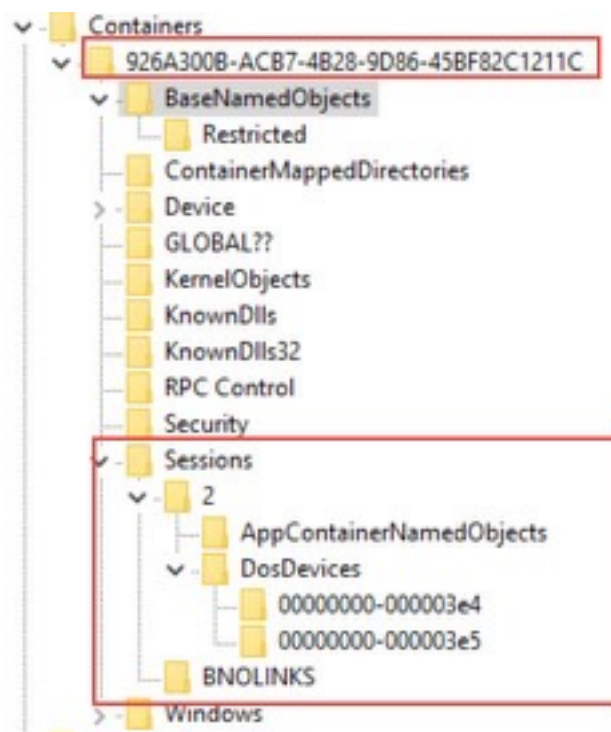
Status Name                DisplayName
-----
Running CExecSvc             Container Execution Agent
Running CoreMessagingRe... CoreMessaging
Running CryptSvc       Cryptographic Services
Running DcomLaunch      DCOM Server Process Launcher
Running Dhcp            DHCP Client
Running Dnscache        DNS Client
Running EventLog        Windows Event Log
Running EventsSystem    COM+ Event System
Running gpvc            Group Policy Client
Running iphlpsvc        IP Helper
Running LanmanWorkstation Workstation
Running LSM             Local Session Manager
Running MSDTC           Distributed Transaction Coordinator
Running nsi             Network Store Interface Service
Running ProfSvc         User Profile Service
Running RpcEptMapper    RPC Endpoint Mapper
Running RpcSs           Remote Procedure Call (RPC)
Running SamSs           Security Accounts Manager
Running Schedule        Task Scheduler
Running SENS            System Event Notification Service
Running SessionEnv      Remote Desktop Configuration
Running sppsvc          Software Protection
Running SystemEventsBroker System Events Broker
Running TermService     Remote Desktop Services
Running Themes          Themes
Running UserManager     User Manager
Running Winmgmt         Windows Management Instrumentation
```

Windows容器如何实现进程间隔离?

类似Session隔离模式



```
PS C:\Users\Administrator> get-container -name psdemo01 | fl id
Id : 926a300b-acb7-4b28-9d86-45bf82c1211c
```



Windows

容器的

Process Explorer - Sysinternals: www.sysinternals.com [DEMO] 192.168.0.4

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Session
winlogon.exe		1,404 K	1,412 K	3160	Windows Logon Application	Microsoft Corporation	3
nvxdsync.exe		5,936 K	10,628 K	3956	NVIDIA User Experience Driver Component	NVIDIA Corporation	3
nvwm64.exe	< 0.01	3,928 K	5,404 K	6132			3
nvsvs.exe	< 0.01	4,056 K	4,520 K	3932	NVIDIA Driver Helper Service, Version 353.24	NVIDIA Corporation	3
LogonUI.exe		15,236 K	15,792 K	5008	Windows Logon User Interface Host	Microsoft Corporation	3
g2tray.exe	0.01	6,644 K	7,188 K	1768	GoToMyPC Host Launcher	Citrix Online, a division of ...	3
dwm.exe		17,304 K	10,184 K	1420	Desktop Window Manager	Microsoft Corporation	3
csrss.exe	< 0.01	2,024 K	1,196 K	3228	Client Server Runtime Process	Microsoft Corporation	3
ChsIME.exe		956 K	1,616 K	5800	Microsoft IME	Microsoft Corporation	3
wininit.exe		896 K	5,232 K	1760	Windows Start-Up Application	Microsoft Corporation	2
svchost.exe		2,272 K	9,272 K	6732	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		1,820 K	6,944 K	5924	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		2,548 K	11,076 K	2688	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		4,544 K	9,660 K	6000	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		11,756 K	28,132 K	5996	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		2,408 K	8,760 K	3340	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		2,016 K	8,080 K	6912	Host Process for Windows Services	Microsoft Corporation	2
svchost.exe		948 K	5,344 K	6972	Host Process for Windows Services	Microsoft Corporation	2
sppsvc.exe		4,528 K	16,248 K	7160	Microsoft Software Protection Platform Service	Microsoft Corporation	2
SppExtComObj.exe		1,424 K	6,976 K	7148	KMS Connection Broker	Microsoft Corporation	2
services.exe		1,848 K	5,892 K	6052	Services and Controller app	Microsoft Corporation	2
msdtc.exe		2,136 K	8,600 K	5580	Microsoft Distributed Transaction Coordinator Service	Microsoft Corporation	2
lsass.exe		2,620 K	10,316 K	3844	Local Security Authority Process	Microsoft Corporation	2
csrss.exe		1,344 K	1,120 K	EE0C	Client Server Runtime Process	Microsoft Corporation	3

Type	Name
ALPC Port	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\RPC Control\LRPC-49437085465bd4f01b
ALPC Port	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\RPC Control\SessEnvPrivateRpc
Desktop	\Default
Directory	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\KnownDlls
Directory	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\TermSrvReadyEvent
Event	\KernelObjects\MaximumCommitCondition
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\SENS Started Event
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\TS Certificate Update Event
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WINMGMT_COREDLL_CANSHTUTDOWN
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WINMGMT_PROVIDER_CANSHTUTDOWN
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WMI_SysEvent_LodCtr
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WMI_SysEvent_UnLodCtr
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WMI_RevAdap_Set
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WMI_RevAdap_ACK
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WMI_ProcessIdleTasksStart
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WMI_ProcessIdleTasksComplete
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\EVENT_READYROOT\CIMV2PROVIDERSUBSYSTEM
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WBEM_ESS_OPEN_FOR_BUSINESS
Event	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\BaseNamedObjects\WINMGMT_PROVIDER_CANSHTUTDOWN

Windows容器如何实现进程间隔离?

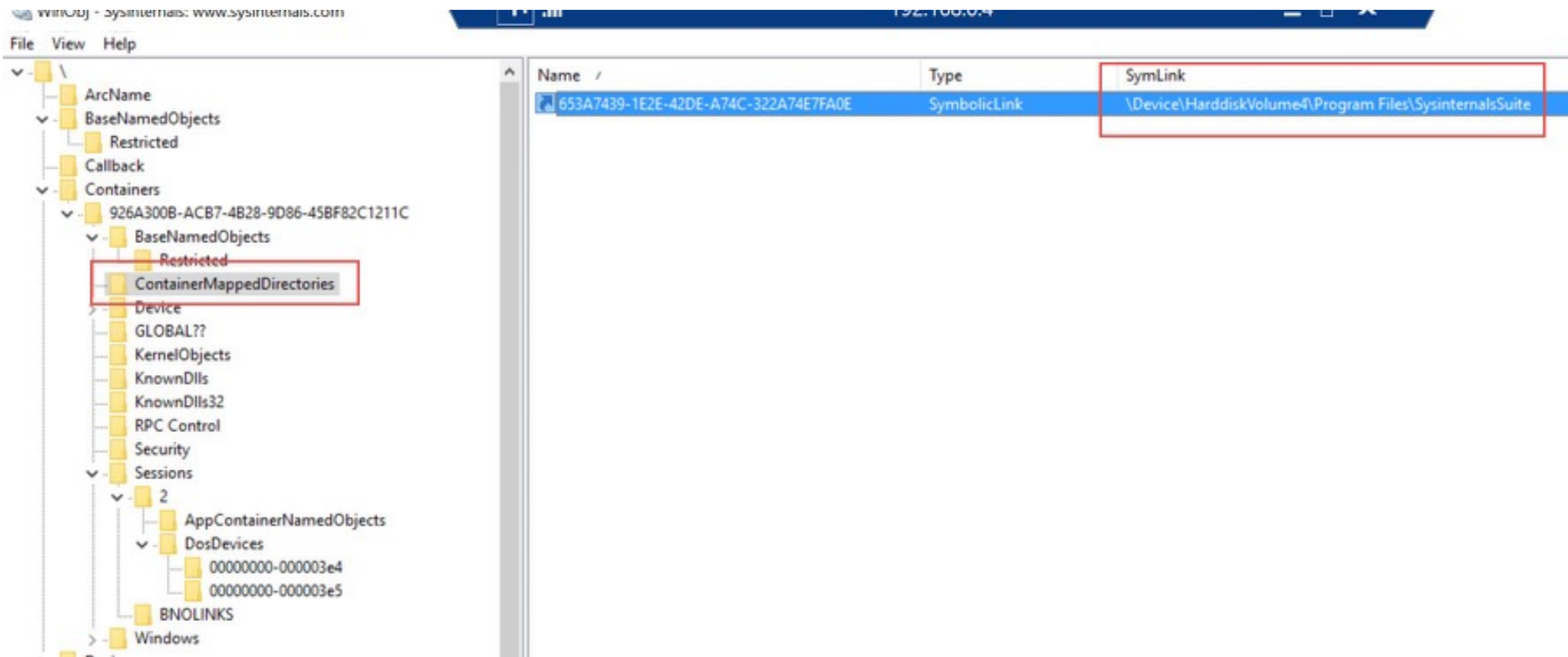
容器进程

svchost.exe	11,756 K	28,132 K	5996 Host Process for Windows Services	Microsoft Corporation	2
svchost.exe	2,408 K	8,760 K	3340 Host Process for Windows Services	Microsoft Corporation	2
svchost.exe	2,016 K	8,080 K	6912 Host Process for Windows Services	Microsoft Corporation	2
svchost.exe	948 K	5,344 K	6972 Host Process for Windows Services	Microsoft Corporation	2
sppsvc.exe	4,528 K	16,248 K	7160 Microsoft Software Protection Platform Service	Microsoft Corporation	2
SppExtComObj.exe	1,424 K	6,976 K	7148 KMS Connection Broker	Microsoft Corporation	2
services.exe	1,848 K	5,892 K	6052 Services and Controller app	Microsoft Corporation	2
msdtc.exe	2,136 K	8,600 K	5580 Microsoft Distributed Transaction Coordinator Service	Microsoft Corporation	2
lsass.exe	2,620 K	10,316 K	3844 Local Security Authority Process	Microsoft Corporation	2
csrss.exe	1,244 K	4,132 K	5596 Client Server Runtime Process	Microsoft Corporation	2
CExecSvc.exe	888 K	4,816 K	6932		2
Winobj.exe	< 0.01	3,928 K	4504 Sysinternals Winobj	Sysinternals	1
winlogon.exe	3,128 K	4,492 K	884 Windows Logon Application	Microsoft Corporation	1

的10
器进

Type	Name
Thread	svchost.exe(5996): 6308
Thread	svchost.exe(5996): 5108
Thread	svchost.exe(5996): 4324
Thread	svchost.exe(5996): 6872
Thread	svchost.exe(5996): 6952
Thread	<Access is denied.>
Thread	svchost.exe(5996): 968
Thread	svchost.exe(5996): 1744
Thread	svchost.exe(5996): 6264
Thread	svchost.exe(5996): 6308
Thread	svchost.exe(5996): 7016
Thread	svchost.exe(5996): 7004
Thread	svchost.exe(5996): 7012
Thread	svchost.exe(5996): 1080
Thread	svchost.exe(5996): 5516
Token	NT AUTHORITY\SYSTEM:3e7
Token	NT AUTHORITY\SYSTEM:3e7
WindowStation	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\Windows\WindowStations\Service-0x0-3e7\$
WindowStation	\Containers\926A300B-ACB7-4B28-9D86-45BF82C1211C\Windows\WindowStations\Service-0x0-3e7\$

Windows容器如何实现进程间隔离?



Windows容器文件系统隔离

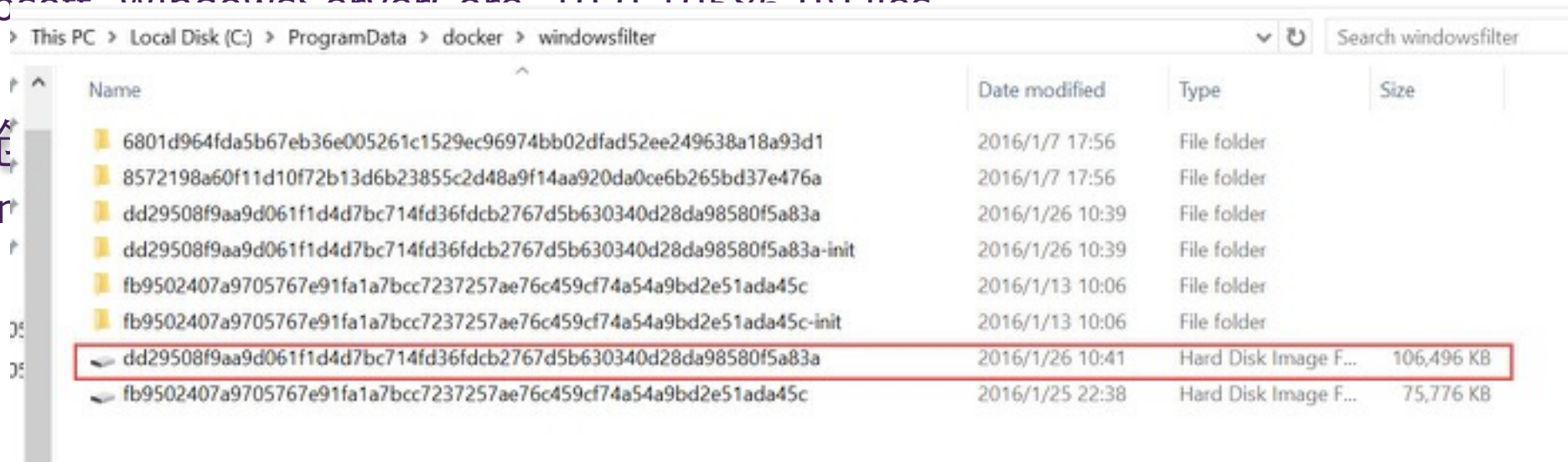
映像文件位于

C:\ProgramData\Microsoft\Windows\Images

\CN=Microsoft-Windows-ServerCore-10.0.10586.0\File...

Dockerfile

C:\Program



This PC > Local Disk (C:) > ProgramData > docker > windowsfilter					Search windowsfilter
Name	Date modified	Type	Size		
6801d964fda5b67eb36e005261c1529ec96974bb02dfad52ee249638a18a93d1	2016/1/7 17:56	File folder			
8572198a60f11d10f72b13d6b23855c2d48a9f14aa920da0ce6b265bd37e476a	2016/1/7 17:56	File folder			
dd29508f9aa9d061f1d4d7bc714fd36fdb2767d5b630340d28da98580f5a83a	2016/1/26 10:39	File folder			
dd29508f9aa9d061f1d4d7bc714fd36fdb2767d5b630340d28da98580f5a83a-init	2016/1/26 10:39	File folder			
fb9502407a9705767e91fa1a7bcc7237257ae76c459cf74a54a9bd2e51ada45c	2016/1/13 10:06	File folder			
fb9502407a9705767e91fa1a7bcc7237257ae76c459cf74a54a9bd2e51ada45c-init	2016/1/13 10:06	File folder			
dd29508f9aa9d061f1d4d7bc714fd36fdb2767d5b630340d28da98580f5a83a	2016/1/26 10:41	Hard Disk Image F...	106,496 KB		
fb9502407a9705767e91fa1a7bcc7237257ae76c459cf74a54a9bd2e51ada45c	2016/1/25 22:38	Hard Disk Image F...	75,776 KB		

Windows容器注册表隔离

和文件系统隔离类似

映像只读部分注册表

C:\ProgramData\Microsoft\Windows\WinSxS

Docker容器的可

docker > windowsfilter > fb9502407a9705767e91fa1a7bcc7237257ae76c459cf74a54a9bd2e51ada45c > Hives

Name	Date modified	Type	Size
<input type="checkbox"/> DefaultUser_Delta	2016/1/19 18:26	File	16 KB
<input type="checkbox"/> Sam_Delta	2016/1/19 18:26	File	64 KB
<input type="checkbox"/> Security_Delta	2016/1/19 18:26	File	32 KB
<input type="checkbox"/> Software_Delta	2016/1/19 18:26	File	128 KB
<input type="checkbox"/> System_Delta	2016/1/19 18:26	File	64 KB

Container Resource Management

Windows



Neil Peterson | Last Updated: 2/23/2016 | 2 Contributors



This is preliminary content and subject to change.

作业对象设定

Process	PID
powershell.exe	4708
java.exe	4784
msdtc.exe	4336

Limit	Value
Job Memory Limit	5,173,248 KB

Network bandwidth limits can be set on an existing container. To do so, ensure the container has a network adapter using the `Get-ContainerNetworkAdapter` command. If a network adapter does not exist, use the `Add-ContainerNetworkAdapter` command to create one. Finally, use the `Set-ContainerNetworkAdapter` command to limit the maximum egress network bandwidth of the container.

The below sample the maximum bandwidth to 100Mbps.

华来四简介

由彭爱华、黄爱华、程尊华和祁清华四个华创建
彭爱华的微信号：markpah，加入我们的微信群

公众号

