



THE CLOUD CONNECTIVITY
COMPANY

Windows on K8S on Windows

Steven Follis and John Jainschigg, Mirantis

San Francisco, CA
APR 2020



You have Windows? We have Questions!

- What's your IT/dev culture and vision?
 - What mix of Windows/Linux do you support today?
 - What mix will you support in 18 months?
- Do your Windows/Linux DevOps/LCM ...
 - Connect/overlap?
 - Evolve discontinuously?
 - Are they portable, e.g., across cloud providers?




You have Windows? We have Questions!

- What's your strategy for containerizing Windows apps?
 - Greenfield (nanoserver-type images)
 - Legacy-friendly (servercore-type images)
 - Heavy/Old-School (windows+32bit images)
- Windows Server version
 - 2019 v. 1903 v. 1909?
 - Process isolation v. Hyper-V isolation?



You have Windows? We have Questions!

- What's your strategy for Kubernetes?
 - Today's reality (K8S 1.17+): mixed Linux + Windows (Worker) clusters
- Things to keep in mind:
 - Windows Server 2019
 - Node selector
 - Lack of privileged containers
 - Linux masters
 - Higher resource needs

The background of the slide is a dark blue field filled with a dense pattern of thin, radiating lines in various shades of blue and red. These lines emanate from the edges of a large, solid black diamond shape that is centered on the slide. The lines create a sense of motion and depth, resembling a stylized starburst or a digital data visualization.

More from
Steven

Aligning pods and nodes

1. Taint nodes to not allow Windows Pods

```
kubectl taint node \  
  [NodeName] beta.kubernetes.io/os=windows:NoSchedule
```

2. Tolerate the taint in PodSpec

```
...  
spec:  
  containers:  
    - name: iis  
      image: iis  
  tolerations:  
    - key: "os"  
      operation: "equal"  
      value: "windows"  
      effect: "NoSchedule"  
  nodeSelector:  
    beta.kubernetes.io/os: windows  
    node.kubernetes.io/windows-build: "10.0.17763"
```



Name: worker01
Labels:
 beta.kubernetes.io/os=linux



Name: worker02
Labels:
 beta.kubernetes.io/os=windows



Name: worker03
Labels:
 beta.kubernetes.io/os=linux

Keep in mind

**Windows
Server
2019**

**node
Selector**

**Lack of
Privileged
Containers**

**Linux
Masters**

**Higher
Resource
Needs
Min 200Mi**

Identity considerations

How do users authenticate to the application?

- Basic Authentication
- Forms Authentication
- Integrate Windows Authentication

How does the application authenticate to resources?

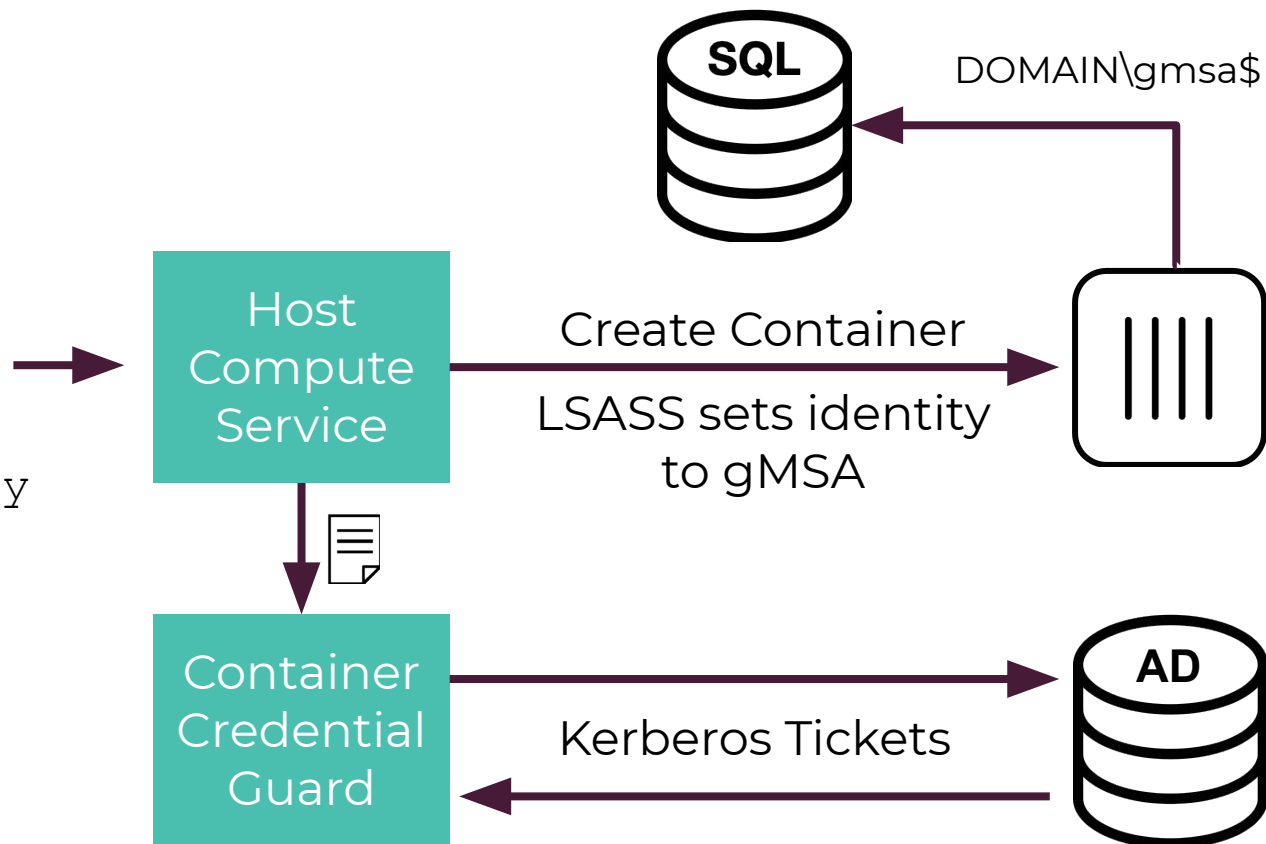
- Can the pod resolve a resource address?
- Is a Group Managed Service Account (gMSA) needed?
- Do worker nodes need to be domain joined?

Using AD with Windows Containers

```
kubectl apply  
docker run  
docker compose up  
docker stack deploy
```

+

 Credential Spec

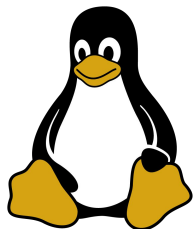


Sample Credential Spec YAML

```
apiVersion: windows.k8s.io/v1alpha1
kind: GMSACredentialSpec
metadata:
  name: gmsa-webapp-1 # used for reference
credspec:
  ActiveDirectoryConfig:
    GroupManagedServiceAccounts:
      - Name: WebApp1 # GMSA account Username
    Scope: CONTOSO # NETBIOS Domain Name
    CmsPlugins:
      - ActiveDirectory
    DomainJoinConfig:
      DnsName: contoso.com # DNS Domain Name
      DnsTreeName: contoso.com # DNS Domain Name Root
      Guid: 244818ae-87ac-4fcd-92ec-e79e5252348a # GUID
      MachineAccountName: WebApp1 # GMSA account Username
      NetBiosName: CONTOSO # NETBIOS Domain Name
      Sid: S-1-5-21-2126449477-2524075714-3094792973 # GMSA SID
```

Logging considerations

Linux Applications



Log to STDOUT

```
➜ docker run -it --rm -p 80:80 nginx:alpine

172.17.0.1 - - [07/Jan/2020:13:17:18 +0000] "GET / HTTP/1.1" 200 161 "-"
OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.4046.105 Safari/537.36
172.17.0.1 - - [07/Jan/2020:13:17:21 +0000] "GET / HTTP/1.1" 200 161 "-"
OS X 10_15_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.4046.105 Safari/537.36
```

Windows Applications

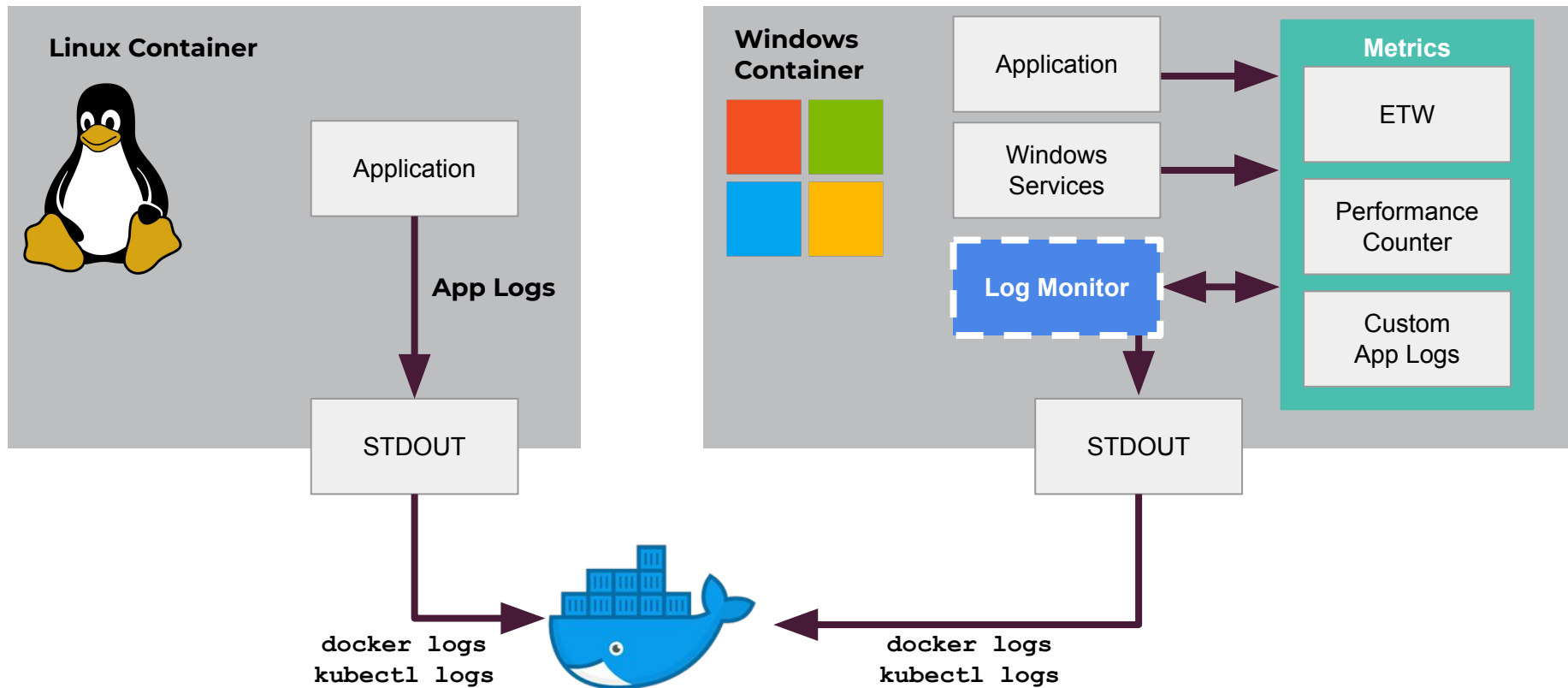


Log to ETW, Event Log, & custom files

```
➜ PS C:\> docker run -it --rm -p 80:80 mcr.microsoft.com/windows/servercore/iis:windowsservercore-ltsc2019

Service 'w3svc' started
```


Using the LogMonitor tool



LogMonitor tool roadmap

- Rotating log support
- Environment variable configuration support
- ConfigMap support
- Integrations with log aggregation services at scale
- Configuration updates during container runtime
- Performance
- Sidecar usage patterns
- Log driver support

Persistent storage considerations

What data is required for your application?

- Is that data persistent?
- How large is the data?
- Databases? File Shares? Local disk locations?

Move towards databases when possible

Extract sensitive values

Identify sensitive components of applications

- Passwords
- Connection Strings
- Certificates

Utilize Kubernetes Secrets

- Clean separate between application and configuration
- RBAC-enabled to ensure proper access

State of K8S storage with Windows

- In-tree and FlexVolume plugins available today
 - File-based cloud volumes
 - Azure File through SMB
 - Block based cloud volumes
 - Azure Disk
 - GCE Persistent Disk
 - AWS EBS (WIP)
 - iSCSI Support (WIP)
- External Provisioners coming soon
- Container Storage Interface (CSI)
 - Becoming the standard for Linux containers
 - Support for Windows is coming but not ready



Thank You

www.mirantis.com/demo