					Connectivity		Access		
Sl.No	Infrastructure Type	Platform		Chaos Agent Deployment Model	Connectivity Requirements from Agent	Connectivity Requirements from WF VM/Cluster/App	Access Requirements For Agent Install	Access Requirements For Basic Chaos Experiments	Access Requirements For Advanced Chaos Experiments
1	On-Premise VMs	VMware VMs	Linux OS	**Native Chaos Agent on Each VM** (systemd-based service within Target Linux Machine)	1. Outbound over port 443 to Harness from VM 2. Outbound to application health endpoints (ones which will be used for resilience validation) from VM	WF Application & Chaos Agent Co-Exist on same VM	Install agent as a root user (one-time)	Run experiments with non-root user	Run experiments with root user
				Centralized Chaos Agent on Kubernetes (leverage VMware Tools to inject chaos processes inside guest VM)	1. Outbound over port 443 to Harness from Kubernetes cluster 2. Outbound over 443 to vCenter from Kubernetes cluster 3. Outbound to application health endpoints (ones which will be used for resilience validation) from kubernetes cluster	1. Inbound over port 443 on ESX Host (from Kubernetes Chaos Agent)	Install agent as a cluster-admin OR as a user mapped to cluster role with these permissions.	vCenter user should be mapped to predefine "chaos" role VMware tools should be setup on the VM Remote command injection can be performed with non-root user	vCenter user should be mapped to predefine "chaos" role VMware tools should be setup on the VM Remote command injection can be performed with root user
			Windows OS	**Native Chaos Agent on Each VM** (system service within Target Windows Machine)	1. Outbound over port 443 to Harness from VM 2. Outbound to application health endpoints (ones which will be used for resilience validation) from VM	WF Application & Chaos Agent Co-Exist on same VM	Install agent as a Administrator user (one-time)	Run experiments with non-administrator user	Run experiments with administrator user
				Centralized Chaos Agent on Kubernetes (leverage VMware Tools to inject chaos processes inside guest VM)	1. Outbound over port 443 to Harness from Kubernetes cluster 2. Outbound over 443 to vCenter from Kubernetes cluster 3. Outbound to application health endpoints (ones which will be used for resilience validation) from kubernetes cluster	1. Inbound over port 443 on ESX Host (from Kubernetes Chaos Agent)	Install agent as a cluster-admin OR as a user mapped to cluster role with these permissions.	vCenter user should be mapped to predefine "chaos" role VMware tools should be setup on the VM Remote command injection can be performed with non-administrator user	vCenter user should be mapped to predefine "chaos" role VMware tools should be setup on the VM Remote command injection can be performed with administrator user
2	Private Cloud	TAS	PCF	**Chaos Agent on Each Diego Cell** (systemd-based service within Diego Cell)	1. Outbound over port 443 to Harness from PCF app container 2. Outbound to application health endpoints (ones which will be used for resilience validation) from VM	WF Application & Chaos Agent Co-Exist on same VM	Install agent as a root user (one-time)	Run experiments with non-root user	Run experiments with root user
				Chaos Agent As PCF App (With Chaos Sidecars) (agent runs as pcf application include chaos sidecar in app containers)	1. Outbound over port 443 to Harness from PCF Chaos Agent app 2. Outbound to application health endpoints (ones which will be used for resilience validation) 3. Inboud over port 8081 from target apps (running chaos sidecar process)	WF Application & Chaos Agent Co-Exist as Apps on the same PCF cluster. However, network policy needs to be setup for the below: 1. Outbound from target apps running chaos sidecar process to the PCF Chaos Agent App	Install agent pcf app and bundle chaos sidecar into target apps as a CF space developer	Run experiments with non-root user	Run experiments with non-root user
				Centralized Chaos Agent on Tanzu Ops Manager (Jumpbox) (systemd-based service within the jumpbox)	1. Outbound over port 443 to Harness from PCF app container 2. Outbound to application health endpoints (ones which will be used for resilience validation) from VM	1. Inbound over port 22 (via cf-ssh) into diego cell from Tanzu Ops Manager / Jumpbox VM	Install agent as a root user (one-time)	Run experiments with non-root user	Run experiments with root user
3	On-Premise K8s	TKGI	Kubernetes	**Centralized Chaos Agent on Kubernetes** (leverage kube-api and container-runtime api to inject faults on K8s microservices)	1. Outbound over port 443 to Harness from Kubernetes cluster 2. Outbound to application health endpoints (ones which will be used for resilience validation) from kubernetes cluster	WF Application & Chaos Agent Co-Exist as pods on the same cluster	Install agent as a cluster-admin OR as a user mapped to cluster role with these permissions.	Chaos ServiceAccount: [consolidated serviceaccount for basic pod chaos] Container Runtime privileges: [None]	Chaos ServiceAccount: [consolidated serviceaccount for advanced pod and node chaos] Container Runtime privileges: [recommended psp for advanced chaos]
4	Public Cloud	AWS	Self-Managed Infra Managed Services	**Centralized Chaos Agent on Kubernetes** (leverage kube-api and container-runtime api to inject faults on K8s microservices)	1. Outbound over port 443 to Harness from Kubernetes cluster 2. Outbound to application health endpoints (ones which will be used for resilience validation) from kubernetes cluster 3. Oubound to Cloud Provider's Public Account Endpoint	No settings needed on the Cloud Target Side	Install agent as a cluster-admin OR as a user mapped to cluster role with these permissions.	AWS: IAM role mapped to [policy for basic aws chaos]	AWS: IAM role mapped to [policy for advanced aws chaos]