**SPOT PC AND AVD REFERENCE ARCHITECTURE**

Azure Virtual Desktop (AVD) requires security accounts and components in both Azure AD and the local Active Directory to perform automated actions. Spot PC creates components and security settings during the deployment process that allow administrators to control the AVD environment. This document describes the relevant Spot PC accounts, components, and security settings in both environments.

**SERVICE DIAGRAM**

### MANAGEMENT CONSTRUCTS

Spot PC deployments live in the customer’s tenant (Azure AD, network, users/groups). The compute, storage and services leveraged by Spot PC run in a subscription generated by NetApp’s CSP account. While the customer must accept a Reseller relationship request from the NetApp CSP account (per Microsoft’s instructions and guidelines [here](#)) in order for NetApp’s subscription to be associated with the customer’s tenant, Spot PC does not require any level of permissions grant via that Reseller relationship request.

**CONFIDENTIALITY:** This document and any analysis, language and proposed concepts or models contained herein remain the exclusive intellectual property of NetApp Corporation (“NetApp”). This document may not be disclosed, reproduced in part or full or otherwise presented to any party but the expressed intended audience and for the expressed purpose without written consent of NetApp. | Revised 3.15.2022
**Spot PC and AVD Reference Architecture**

Resources and components defined here are separated by whether they reside in the customer tenant or within the CSP-generated subscription.

**Customer Tenant**

The following Spot PC elements reside strictly in the customer tenant (but outside of the NetApp CSP subscription/resource group). – they are typically related to Enterprise Applications, App Registrations, Azure Active Directory and networking.

- **Azure AD Enterprise Applications** - Spot PC leverages Enterprise Applications and App Registrations in a tenant's Azure AD domain. The Enterprise Applications are the conduit for the calls against the Azure Resource Manager and Azure Graph using the delegated roles and permissions granted to the associated Service Principal. App registrations may be created depending on initialization state of AVD services for the tenant through Spot PC:
  - **Spot PC Discovery** – This temporary enterprise application is the initial Enterprise Application admins grant consent to and is used during the Spot PC wizard-driven deployment process. This is automatically removed once it is no longer required.
  - **Spot PC** – Handles general management calls for Azure PaaS functions. Examples of Azure PaaS functions are Azure Compute, Azure NetApp Files, Azure Files, etc. as well as making calls to the Graph API. This Service Principal requires Owner rights to the target (NetApp-owned) Azure subscription during initial deployment.

- **Azure Virtual Network and Subnets** – Spot PC discovers existing networks available and presents them as choices during various workflows. Customers authorize VNet peering between their existing network and the Spot PC network during the onboarding wizard.

**NetApp CSP Subscription**

The following Spot PC elements reside inside a NetApp subscription/resource group associated with the customer tenant. They are typically PaaS services and Compute and Storage resources required for the Spot PC platform and AVD host pools.

**Azure Components and Security Settings**

AVD requires that the user session Virtual Machines (VM) be created in an Azure subscription. To enable the creation and management of these VMs, Spot PC creates several supporting components in the Azure Subscription:

- **Azure Resource Group** – Spot PC creates an Azure Resource Group to contain the other AVD components, including VMs, network subnets, network security groups, and either Azure Files containers or Azure NetApp Files capacity pools.

- **Azure Virtual Network and Subnets** – Spot PC creates an Azure Virtual Network and supporting subnets. Spot PC requires a separate subnet for SpotManager1, AVD host machines, and Azure domain controllers and peering between the subnets. Note that the AD controller subnet typically already exists so the Spot PC deployed network will need to be peered with the existing network.

**Confidentiality:** This document and any analysis, language and proposed concepts or models contained herein remain the exclusive intellectual property of NetApp Corporation (“NetApp”). This document may not be disclosed, reproduced in part or full or otherwise presented to any party but the expressed intended audience and for the expressed purpose without written consent of NetApp. | Revised 3.15.2022
**SPOT PC AND AVD REFERENCE ARCHITECTURE**

- **Azure Cosmos DB** – Spot PC leverages Cosmos database services inside the region/s in which the customer elects to deploy them. Keeping the Cosmos database in the customer tenant allows nearly all data to reside in the region/s the customer desires.

- **SpotManager1** – SpotManager1 is the local control plane VM for each Deployment. By default, it is created as a Windows 2019 Server VM in the target Azure subscription. See the Local Deployment section for the list of Spot PC and 3rd party components installed on SpotManager1.

- **Service Bus** – Spot PC uses the Service Bus to publish/subscribe to updates to securely (without open ports) and reliably broker commands between:
  - Spot PC Orchestration Container (on SpotManager1) and the Global Control Plane
  - The Spot PC Agent and the Spot PC Orchestration Container (on SpotManager1)

- **Network Security Group (NSG)** – a network security group is created to control access to the SpotManager1 VM.
  - Tenant: contains IP addresses for use by session host and database VMs
  - Services: contains IP addresses for use by PaaS services (Azure NetApp Files, for example)
  - Platform: contains IP addresses for use as NetApp platform VMs (SpotManager1)
  - Directory: contains IP addresses for use as Active Directory VMs
    - Note: Directory subnet is only used if the customer elects to leverage AADDS or a newly created AD VM.
  - Container: contains IP addresses for use by the Spot PC Orchestration Container

- **Azure NetApp Files Capacity Pool (50+ user deployments)** – an Azure NetApp Files Capacity Pool and associated Volume(s) will be created if your deployment consists of 25 users or more. The Capacity pool contains at least 1 Volume that hosts the shared file storage for user profiles (via FSLogix containers), user personal folders and the corporate data share folder.

- **Azure File Share (deployments with fewer than 50 users)** – an Azure File Share and its associated Azure Storage Account will be created for deployments with fewer than 25 users. The Azure File Share hosts the shared file storage for user profiles (via FSLogix containers), user personal folders and the corporate data share folder.

- **Database/Business Server (Optional)** – one or more Windows Server VMs can be provisioned for general purposes or to house SQL databases for client/server applications.

- **Recovery Service Vault (Optional)** – a Recovery Service Vault is created by Spot PC Automation during deployment. This is currently activated by default, as Azure Backup is applied to SpotManager1 during the deployment process.

- **Key Vault** – an Azure Key Vault is created during the deployment process and is used to store certificates, API keys and credentials that are used by Spot PC during deployment.

- **Automation account** – an Automation account is created during deployment and is a required component during the provisioning process. The Automation account contains variables, credentials, modules and Desired State Configurations and references the Key Vault.
  - Desired State Configuration: this is the method used to build SpotManager1 (and optionally, a new AD VM if desired) as well as maintain the configuration of SpotManager1 (no other VMs, unless the customer elects to use a newly created AD VM for Spot PC – in which case this would apply to that VM as well). The configuration file is downloaded to the Spotmanager1 VM and applied via a Microsoft service on the
SPOT PC AND AVD REFERENCE ARCHITECTURE

VM. The configuration file checks for updates daily and enforces the configuration twice daily. Examples of configuration elements include:

- Ensuring the proper permission sets are applied
- Ensuring required software components are installed
- Ensuring that SpotManager1 is joined to the domain

- **Log Analytics** – a Log Analytics workspace is created to store logs from the Spot PC environment and from other sources, such as AVD logins. This can be deleted after deployment, but this isn’t recommended as it enables other functionality. Logs are retained for 30 days by default, incurring no charges for retention.

- **Availability Set** – an Availability Set is set up as a part of the deployment process to enable separation of shared VMs (shared AVD host pools) across fault domains. This can be deleted after deployment if desired, but would disable the option to provide additional fault tolerance for shared VMs.

Note that Azure Virtual Desktop also installs Azure components, including Enterprise Applications and App Registrations for Azure Virtual Desktop and Azure Virtual Desktop Client, the AVD Tenant, AVD Host Pools, AVD App Groups, and AVD registered Virtual Machines. While Spot PC Automation components manage these components, AVD controls their default configuration and attribute set so refer to the AVD documentation for details.

Azure Subscription Roles and Delegated Permissions

The Enterprise Applications and App Registrations below are created request a set of roles/permissions following the “least required” methodology during the Spot PC onboarding process. These permissions are used for interactions with Cloud PC controls as well as Threat and Vulnerability Management

- **Spot PC Discovery Enterprise Application** (note: only if connecting to an existing AD environment)
- **Spot PC App Registration**
- **Cloud Workspace API Enterprise Application**

Local Deployment (Azure Subscription) Components

AVD requires the AVD VMs be joined to an Active Directory domain. To facilitate this process and to provide the automation tools for managing the Spot PC environment several components are installed on the SpotManager1 VM described above and several components are added to the AD instance. The components include:

- **Windows Services** – Spot PC uses Windows services to perform automation and management actions from within a deployment:
  
  - **Spot PC Orchestration Container (SPOC)** is a Windows Service deployed on SpotManager1 in each AVD deployment that performs many of the user-facing automation tasks in the environment. This service runs under the CloudWorkspaceSVC AD account. SPOC also performs the virtual machine management functions. This service runs under the CloudWorkspaceSVC AD account.
  
  - **Spot PC Agent Service** is a Windows Service deployed to each virtual machine under Spot PC management, including SpotManager1. This service runs under the LocalSystem context on the virtual machine.
SPOT PC AND AVD REFERENCE ARCHITECTURE

- **HTML5 Portal (Optional)** – Spot PC installs the Myrtille service (a .NET framework based application) to provide HTML5 access to VMs from the Spot PC web application.

- **Spot PC Command Center** – this is an .aspx application used to perform Deployment and Spot PC Site specific configuration and advanced and management tasks in scenarios where API or Web Application tasks need to be modified.

Spot PC also requires several Active Directory components to support the Automation tasks. The design intent is to utilize a minimum number of AD component and permission additions while still supporting the require environment for automated management. These components include:

- **Spot PC Organizational Unit (OU)** – this Organization Unit will act as the primary AD container for the required child components. Permissions for the spotpc-Infrastructure and Client DHP Access groups will be set at this level and its child components. See Appendix B for sub-OUs that are created in this OU.

- **Spot PC Infrastructure Group** (<code>spotpc-Infrastructure</code>) is a security group created in the local AD to allow required delegated permissions to be assigned to the Spot PC service account (<code>SpotPCManagerSvcAcc</code>)

- **Client DHP Access Group** (<code>ClientDHPAccess</code>) is a security group created in the local AD to allow Spot PC to govern the location in which the company shared, user home and profile data reside.

- **SpotPCManagerSvcAcc** is a service account (member of spotpc-Infrastructure Group) leveraged to process automation actions

- **Level3 Technicians** is a group that houses users that have temporarily been granted admin privileges

*Note that the Default Group Policy setting configurations can be provided on request.*

APPENDIX A: AVD VIRTUAL MACHINE CREATION

The Spot PC automation and orchestration deploys virtual machines into a targeted Active Directory instance and then joins the machines to the designated host pool. AVD virtual machines are governed at a computer level by both the AD structure (organizational units, group policy, local computer administrator permissions etc.), and membership in the AVD structure (host pools, app group membership), which governed by Azure AD entities and permissions. Spot PC handles this “dual control” environment by using the Spot PC Enterprise application/Azure Service Principal for AVD actions and the local AD service account (<code>SpotPCManagerSvcAcc</code>) for local AD and local computer actions.

The specific steps for creating an AVD virtual machine and adding it to the AVD host pool include:

- Create Virtual Machine from Azure template visible to the Azure Subscription associated with AVD (uses Azure Service Principal permissions)

- Check/Configure DNS address for new Virtual Machine using the Azure VNet designated during Spot PC Deployment (requires local AD permissions (everything delegated to spotpc-Infrastructure above)) Sets the Virtual Machine name using the standard Spot PC naming scheme (companycode)TS(sequencenumber). Example: XYZTS3. (Requires local AD permissions (placed into OU structure we have created on-prem (remote desktop/companycode/shared) (same permission/group description as above)

- Places virtual machine in designated Active Directory Organizational Unit (AD) (requires the delegated permissions to the OU structure (designated during manual process above))

- Update internal AD DNS directory with the new machine name/ IP address (requires local AD permissions)

- Join new virtual machine to local AD domain (requires local AD permissions)

**CONFIDENTIALITY:** This document and any analysis, language and proposed concepts or models contained herein remain the exclusive intellectual property of NetApp Corporation (“NetApp”). This document may not be disclosed, reproduced in part or full or otherwise presented to any party but the expressed intended audience and for the expressed purpose without written consent of NetApp. | Revised 3.15.2022
**SPOT PC AND AVD REFERENCE ARCHITECTURE**

- Update Spot PC local database with new server information (does not require additional permissions)
- Join VM to designated AVD Host Pool (requires AVD Service Principal permissions)
- Install Chocolatey components to the new Virtual Machine (requires local computer administrative privilege for the SpotPCMangerSvcAcc account)
- Install FSLogix components for the AVD instance (Requires local computer administrative permissions on the AVD OU in the local AD)
- Set “Allow New Connections” flag on the new virtual machine (requires Azure Service Principal permissions)

**APPENDIX B – SPOT PC ORGANIZATIONAL UNIT STRUCTURE**

- Spot PC
  - Computers
    - Remote Desktop
      - Pooled Session Host Servers
      - Personal Session Host Servers
    - Users
  - Users