Azure – Landing Zone

Cloud Computing

6/9/2020
Data Communications Labs
Tony Shen

Contents

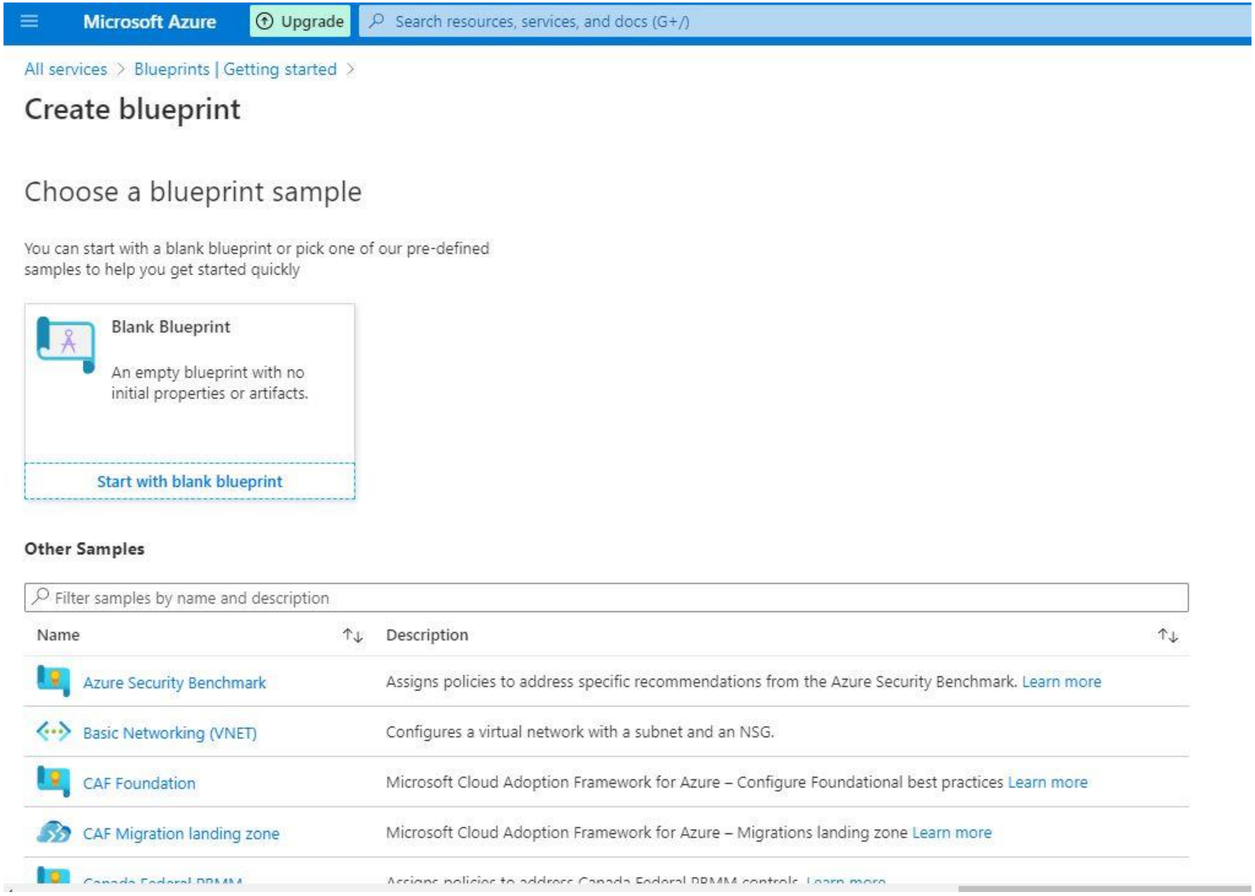
Introduction

Azure Landing Zone (ALZ) is a new feature in Azure cloud designed to facilitate resource creation and configuration standardization. ALZ uses blueprints to do its work. This write-up provides a walk-through of creating resources by using a blueprint to illustrate how it works. The walk-through includes basic steps of creating, drafting, publishing and assigning a blueprint. Desired resources are created by assigning a published blueprint to targeted areas. A blueprint cannot be published until it is carefully drafted. When drafting a blueprint, built-in guard-rails are in place to prevent non-conforming practices from taking place. The entire process from drafting, publishing, and assigning blueprints ensures an enterprise-grade standardization, consistency, and best practices across board.

Walk-through

Drafting a blueprint

Figure 1 - Creating a blueprint by choosing a sample



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
All services > Blueprints | Getting started >

Create blueprint

Choose a blueprint sample

You can start with a blank blueprint or pick one of our pre-defined samples to help you get started quickly

Blank Blueprint

An empty blueprint with no initial properties or artifacts.

Start with blank blueprint

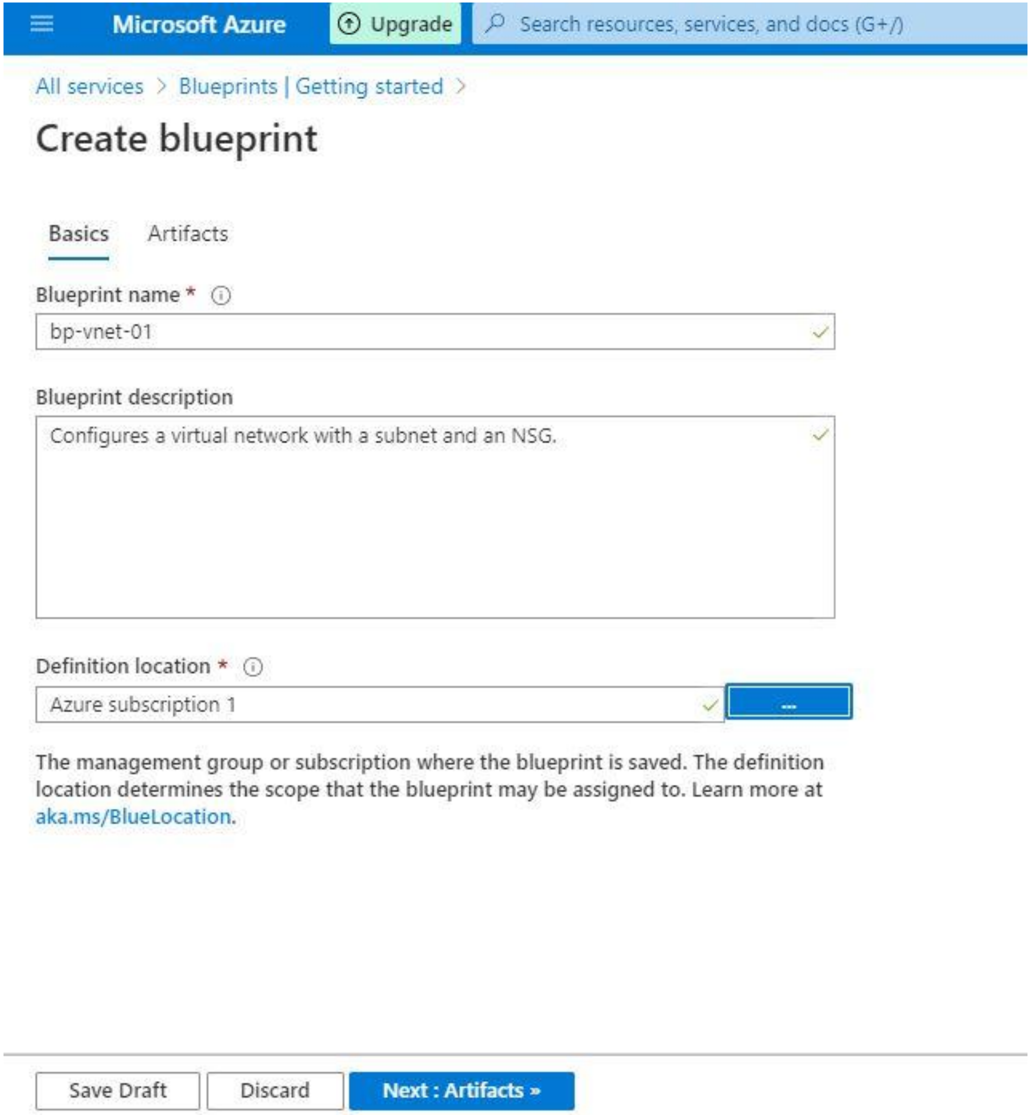
Other Samples

Filter samples by name and description

Name ↑↓	Description ↑↓
Azure Security Benchmark	Assigns policies to address specific recommendations from the Azure Security Benchmark. Learn more
Basic Networking (VNET)	Configures a virtual network with a subnet and an NSG.
CAF Foundation	Microsoft Cloud Adoption Framework for Azure – Configure Foundational best practices Learn more
CAF Migration landing zone	Microsoft Cloud Adoption Framework for Azure – Migrations landing zone Learn more
Canada Federal PBMM	Assigns policies to address Canada Federal PBMM controls. Learn more

In this walk-through, Basic Networking (VNET) was chosen

Figure 2 – Naming the blueprint



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
All services > Blueprints | Getting started >

Create blueprint

Blueprint name * : bp-vnet-01

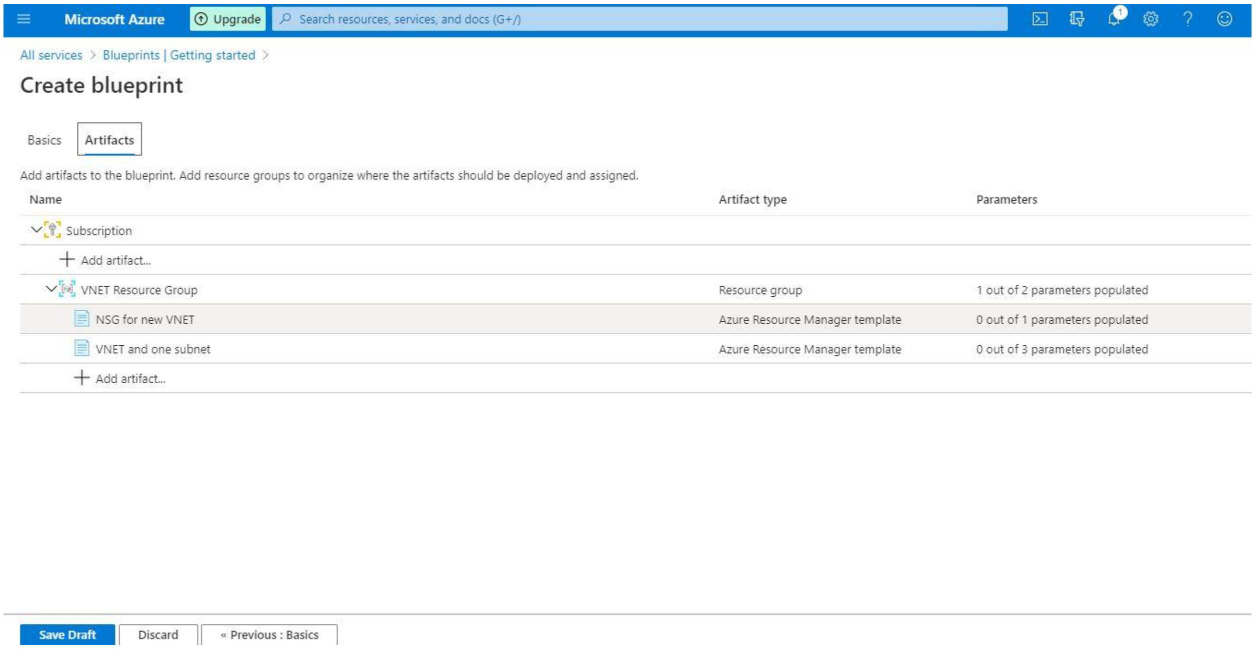
Blueprint description: Configures a virtual network with a subnet and an NSG.

Definition location * : Azure subscription 1

The management group or subscription where the blueprint is saved. The definition location determines the scope that the blueprint may be assigned to. Learn more at aka.ms/BlueLocation.

...
Save Draft
Discard
Next : Artifacts »

Figure 3 – NSG (Network Security Group) and Subnet are added

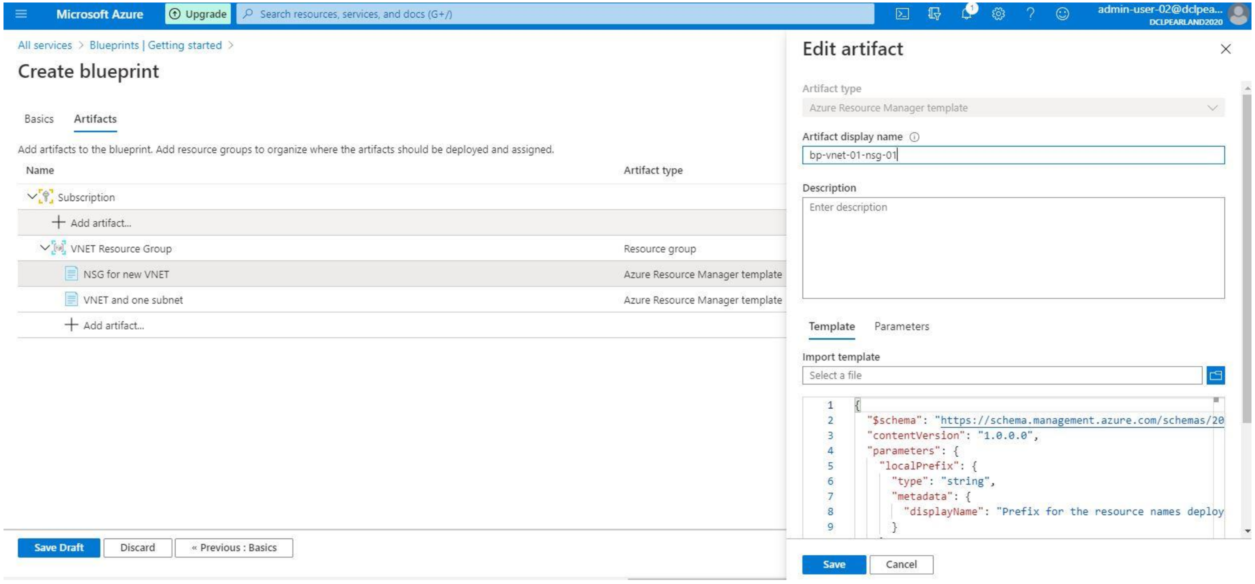

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
All services > Blueprints | Getting started >
Basics
Artifacts
Save Draft
Discard
« Previous : Basics

Create blueprint

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type	Parameters
Subscription		
+ Add artifact...		
VNET Resource Group	Resource group	1 out of 2 parameters populated
NSG for new VNET	Azure Resource Manager template	0 out of 1 parameters populated
VNET and one subnet	Azure Resource Manager template	0 out of 3 parameters populated
+ Add artifact...		

Figure 4 – Naming NSG



Create blueprint

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type
Subscription	
+ Add artifact...	
VNET Resource Group	Resource group
NSG for new VNET	Azure Resource Manager template
VNET and one subnet	Azure Resource Manager template
+ Add artifact...	

Edit artifact

Artifact type: Azure Resource Manager template

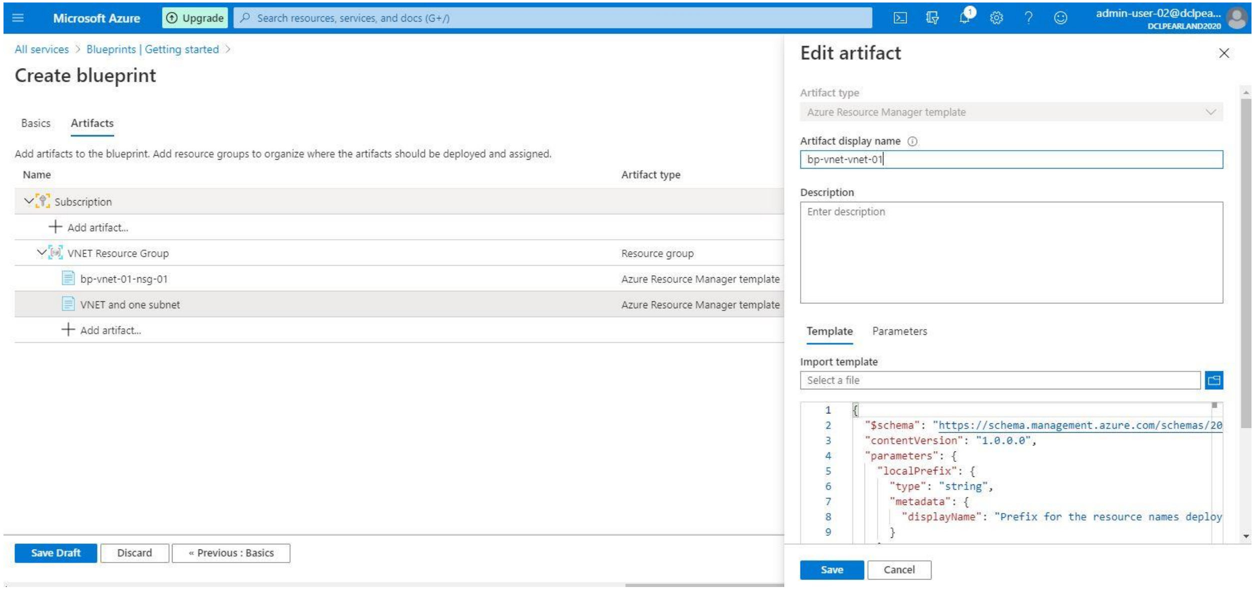
Artifact display name: bp-vnet-01-nsg-01

Description: Enter description

Import template: Select a file

```
{
  "$schema": "https://schema.management.azure.com/schemas/20
  "contentVersion": "1.0.0.0",
  "parameters": {
    "localPrefix": {
      "type": "string",
      "metadata": {
        "displayName": "Prefix for the resource names deploy
      }
```

Figure 5 – Naming VNET



All services > Blueprints | Getting started >

Create blueprint

Basics **Artifacts**

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type
Subscription	
+ Add artifact...	
VNET Resource Group	Resource group
bp-vnet-01-nsg-01	Azure Resource Manager template
VNET and one subnet	Azure Resource Manager template
+ Add artifact...	

Save Draft | Discard | « Previous : Basics

Edit artifact

Artifact type: Azure Resource Manager template

Artifact display name: bp-vnet-vnet-01

Description: Enter description

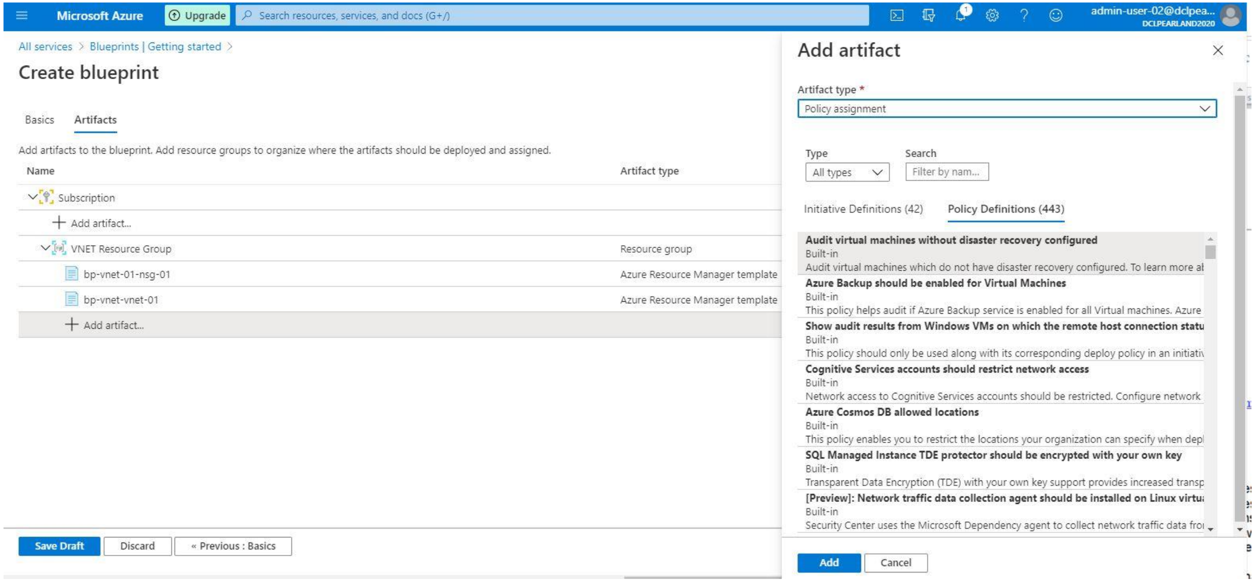
Template Parameters

Import template: Select a file

```
{
  "$schema": "https://schema.management.azure.com/schemas/20
  "contentVersion": "1.0.0.0",
  "parameters": {
    "localPrefix": {
      "type": "string",
      "metadata": {
        "displayName": "Prefix for the resource names deploy
      }
```

Save | Cancel

Figure 6 – Adding a policy



All services > Blueprints | Getting started >

Create blueprint

Basics **Artifacts**

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type
Subscription	
+ Add artifact...	
VNET Resource Group	Resource group
bp-vnet-01-nsg-01	Azure Resource Manager template
bp-vnet-vnet-01	Azure Resource Manager template
+ Add artifact...	

Save Draft | Discard | « Previous : Basics

Add artifact

Artifact type *: Policy assignment

Type: All types

Search: Filter by nam...

Initiative Definitions (42) | **Policy Definitions (443)**

Audit virtual machines without disaster recovery configured
Built-in
Audit virtual machines which do not have disaster recovery configured. To learn more al

Azure Backup should be enabled for Virtual Machines
Built-in
This policy helps audit if Azure Backup service is enabled for all Virtual machines. Azure

Show audit results from Windows VMs on which the remote host connection statu
Built-in
This policy should only be used along with its corresponding deploy policy in an initiativ

Cognitive Services accounts should restrict network access
Built-in
Network access to Cognitive Services accounts should be restricted. Configure network

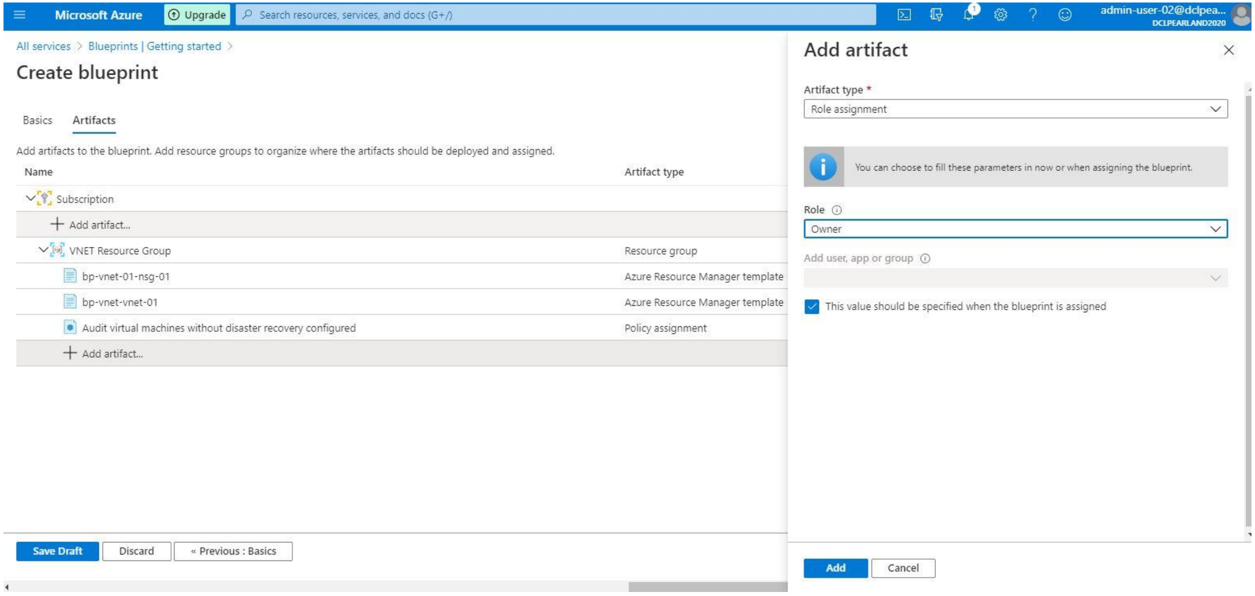
Azure Cosmos DB allowed locations
Built-in
This policy enables you to restrict the locations your organization can specify when depl

SQL Managed Instance TDE protector should be encrypted with your own key
Built-in
Transparent Data Encryption (TDE) with your own key support provides increased transp

[Preview]: Network traffic data collection agent should be installed on Linux virtu
Built-in
Security Center uses the Microsoft Dependency agent to collect network traffic data fro

Add | Cancel

Figure 7 – Adding a role


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
admin-user-02@dclpea...
DCLPEARLAND2020
All services > Blueprints | Getting started >

Create blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type
Subscription	
+ Add artifact...	
VNET Resource Group	Resource group
bp-vnet-01-nsg-01	Azure Resource Manager template
bp-vnet-vnet-01	Azure Resource Manager template
Audit virtual machines without disaster recovery configured	Policy assignment
+ Add artifact...	

Add artifact

Artifact type *: Role assignment

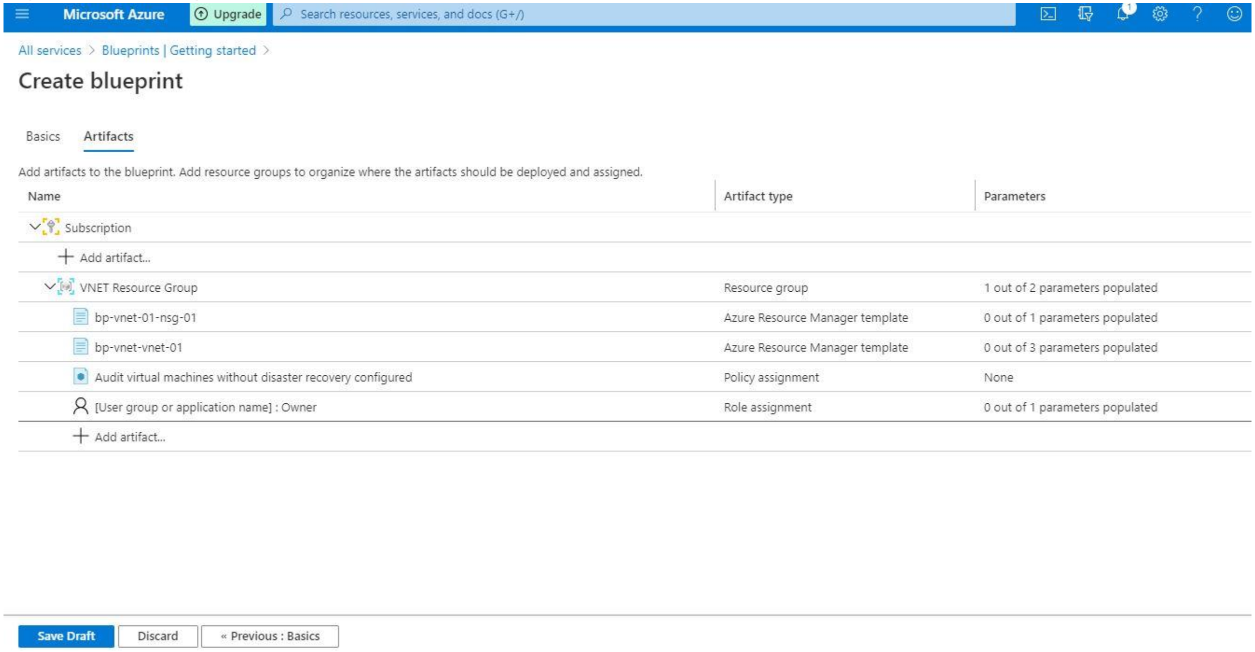
You can choose to fill these parameters in now or when assigning the blueprint.

Role: Owner

Add user, app or group

☑ This value should be specified when the blueprint is assigned

Figure 8 – Saving the draft


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
All services > Blueprints | Getting started >

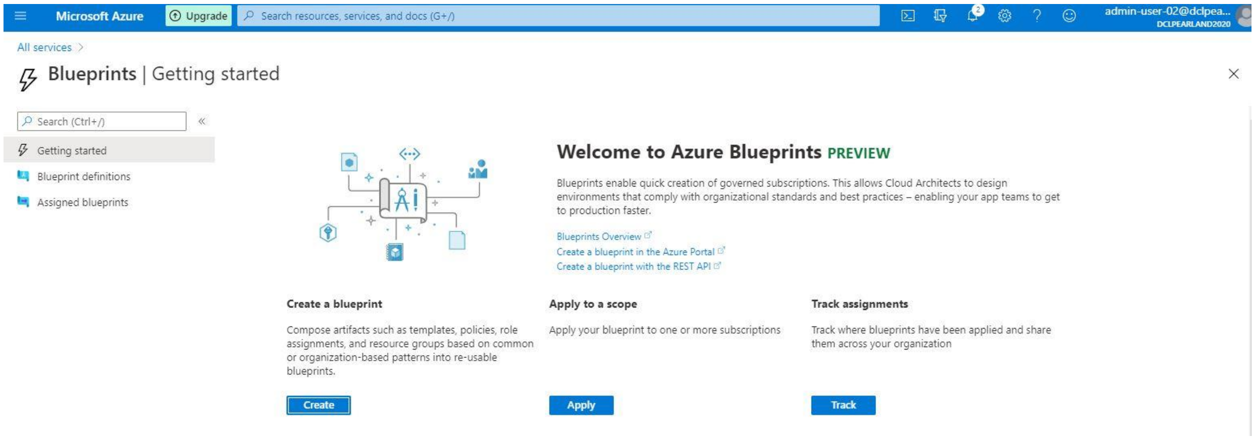
Create blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type	Parameters
Subscription		
+ Add artifact...		
VNET Resource Group	Resource group	1 out of 2 parameters populated
bp-vnet-01-nsg-01	Azure Resource Manager template	0 out of 1 parameters populated
bp-vnet-vnet-01	Azure Resource Manager template	0 out of 3 parameters populated
Audit virtual machines without disaster recovery configured	Policy assignment	None
[User group or application name] : Owner	Role assignment	0 out of 1 parameters populated
+ Add artifact...		

Figure 9 – The draft blueprint is saved in Blueprint definitions



Welcome to Azure Blueprints PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

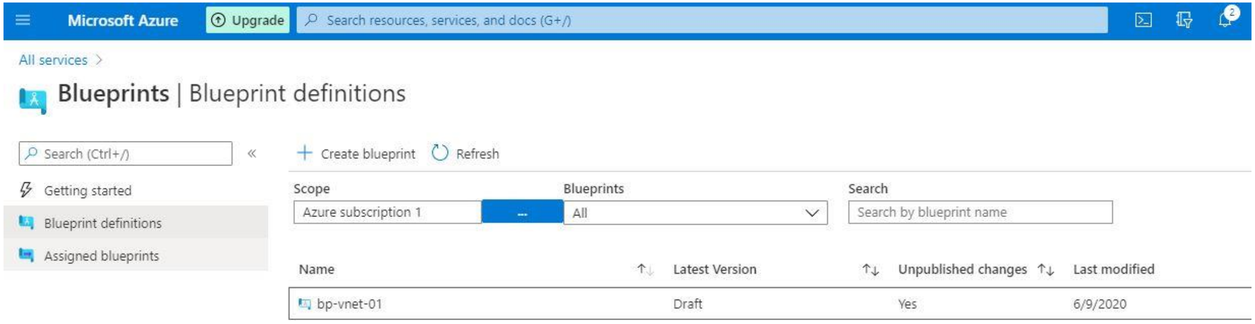
Apply to a scope

Apply your blueprint to one or more subscriptions

Track assignments

Track where blueprints have been applied and share them across your organization

Figure 10 – The saved draft blueprint shows up



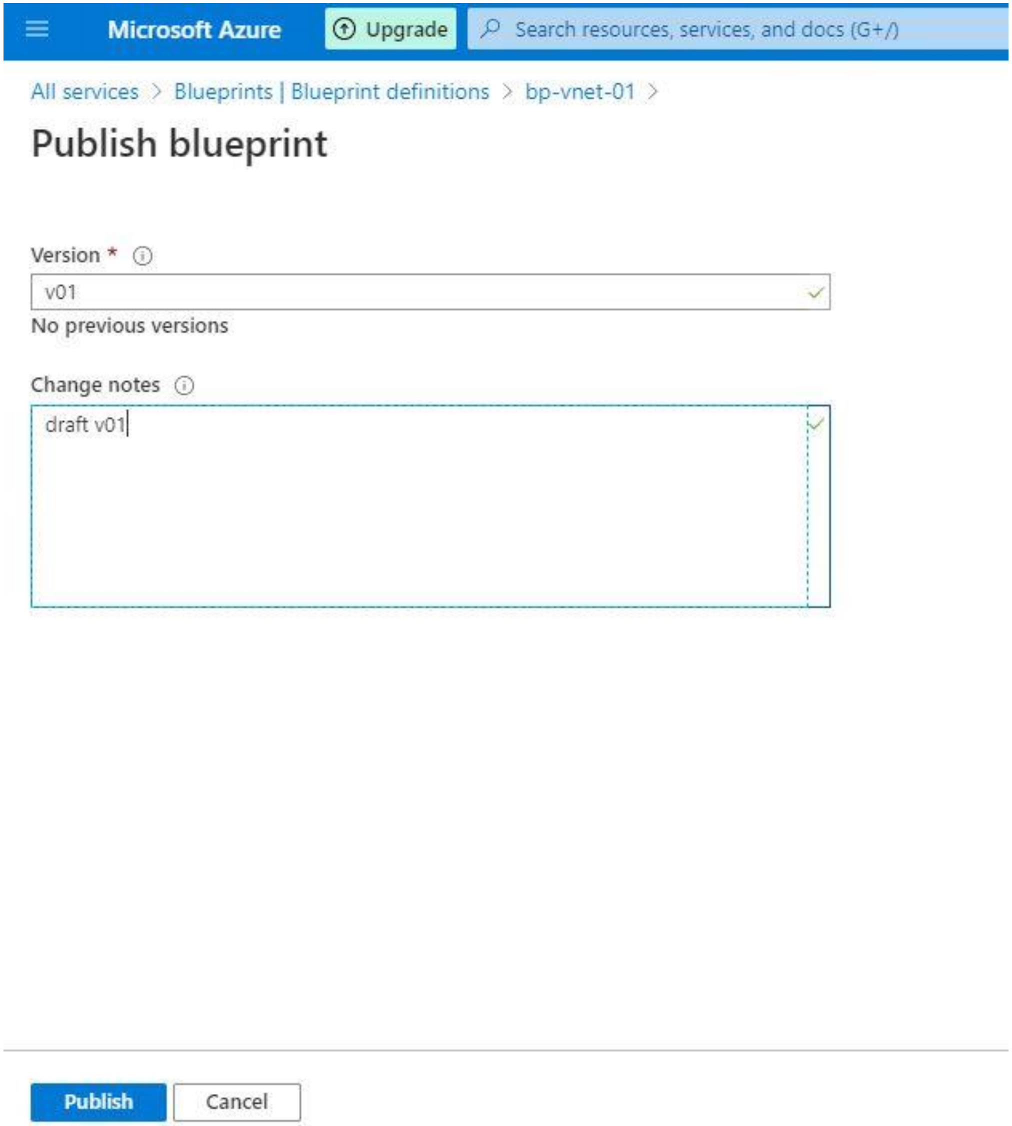
Scope: Azure subscription 1

Blueprints: All

Name	Latest Version	Unpublished changes	Last modified
bp-vnet-01	Draft	Yes	6/9/2020

Publishing blueprint

Figure 11 – Naming a version before publishing the draft blueprint



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
All services > Blueprints | Blueprint definitions > bp-vnet-01 >

Publish blueprint

Version *

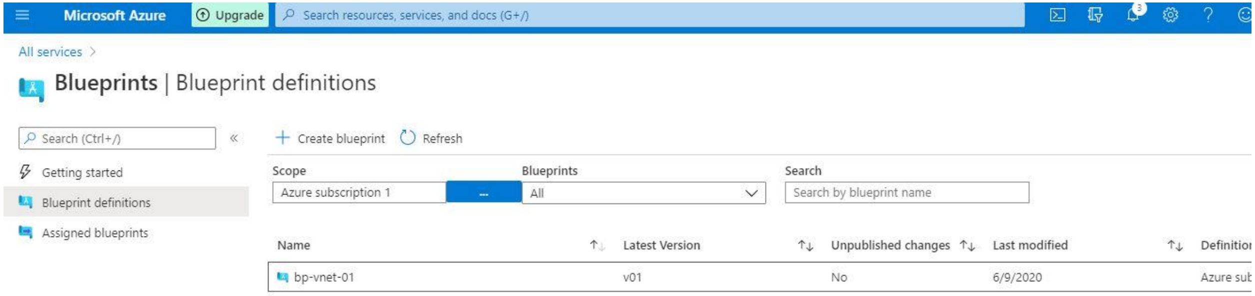
v01

No previous versions

Change notes

draft v01

Figure 12 – The blueprint is versioned and published



Blueprints | Blueprint definitions

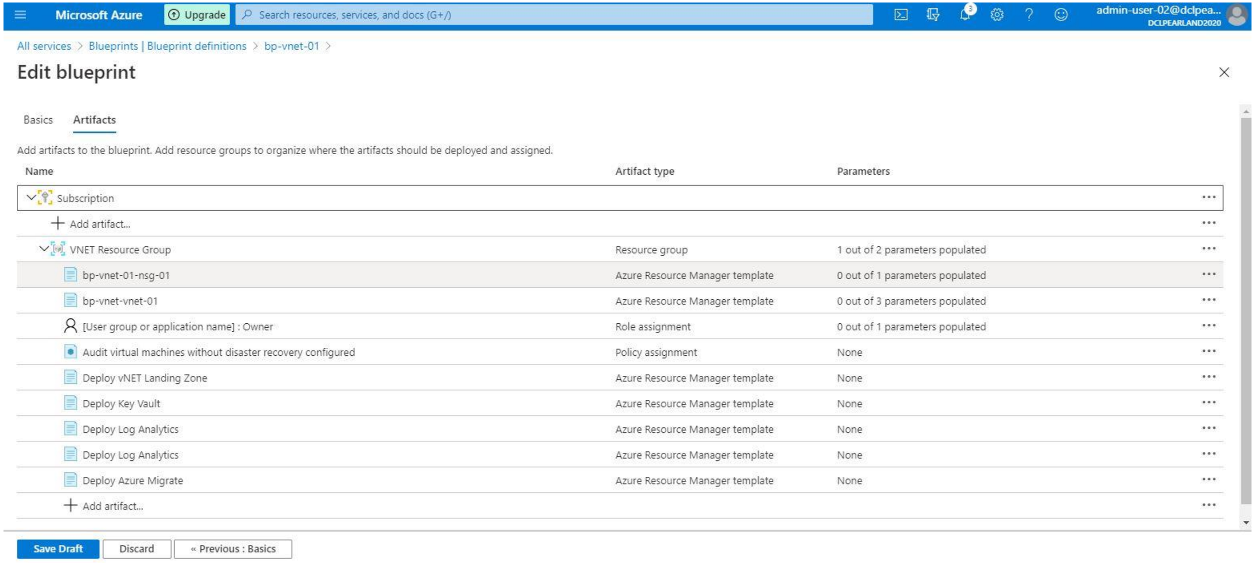
Scope: Azure subscription 1

Blueprints: All

Search: Search by blueprint name

Name	Latest Version	Unpublished changes	Last modified	Definitio
bp-vnet-01	v01	No	6/9/2020	Azure sub

Figure 13 – More artifacts can be added to the blueprint



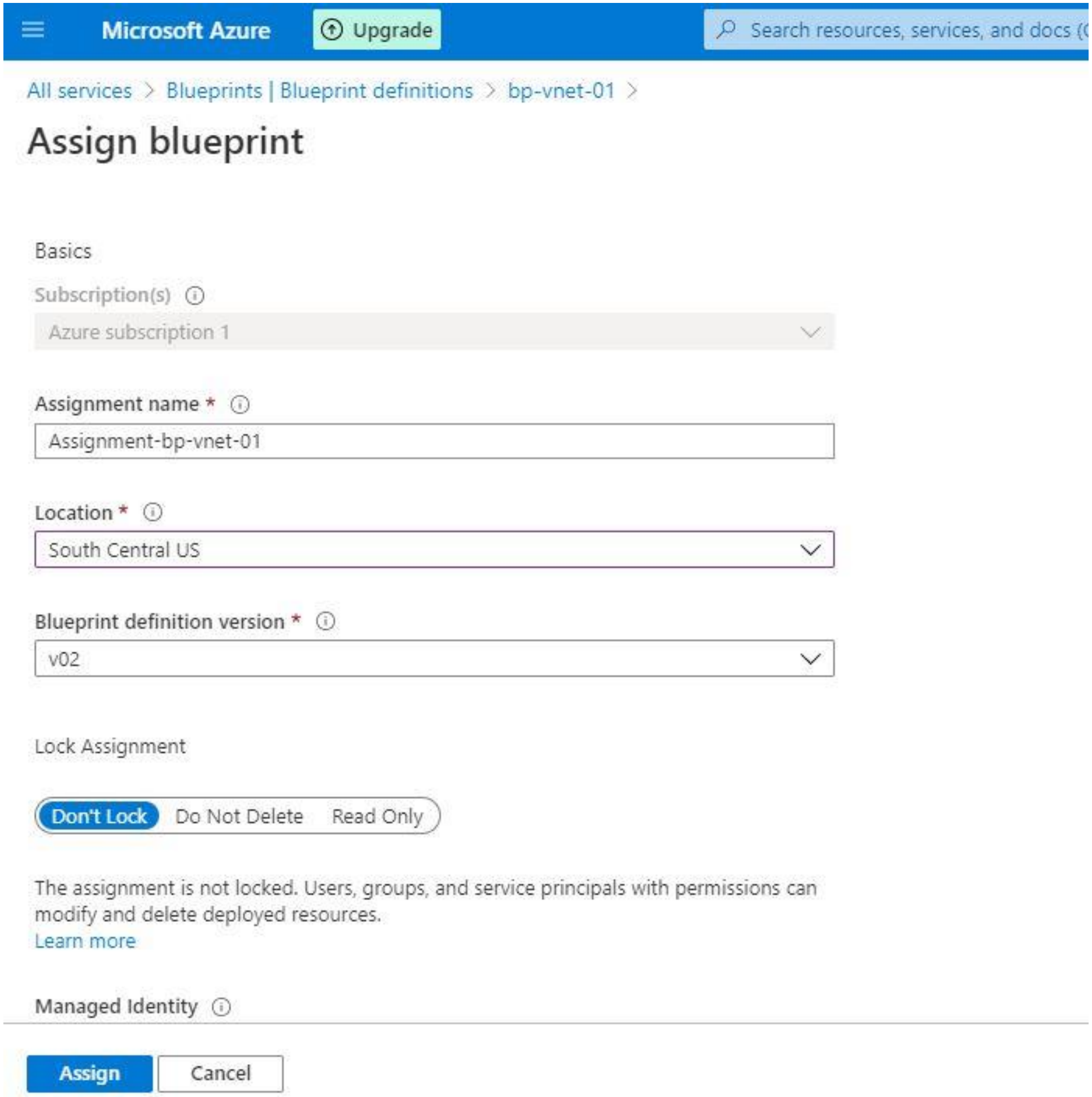
Edit blueprint

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

Name	Artifact type	Parameters
Subscription		
Add artifact...		
VNET Resource Group	Resource group	1 out of 2 parameters populated
bp-vnet-01-nsg-01	Azure Resource Manager template	0 out of 1 parameters populated
bp-vnet-vnet-01	Azure Resource Manager template	0 out of 3 parameters populated
[User group or application name] : Owner	Role assignment	0 out of 1 parameters populated
Audit virtual machines without disaster recovery configured	Policy assignment	None
Deploy vNET Landing Zone	Azure Resource Manager template	None
Deploy Key Vault	Azure Resource Manager template	None
Deploy Log Analytics	Azure Resource Manager template	None
Deploy Log Analytics	Azure Resource Manager template	None
Deploy Azure Migrate	Azure Resource Manager template	None
Add artifact...		

Assigning blueprint

Figure 14 – Assigning the blueprint (using the blueprint to create resources)


Microsoft Azure
Upgrade
Search resources, services, and docs (
All services > Blueprints | Blueprint definitions > bp-vnet-01 >
Assign, Cancel

Assign blueprint

Basics

Subscription(s): Azure subscription 1

Assignment name *: Assignment-bp-vnet-01

Location *: South Central US

Blueprint definition version *: v02

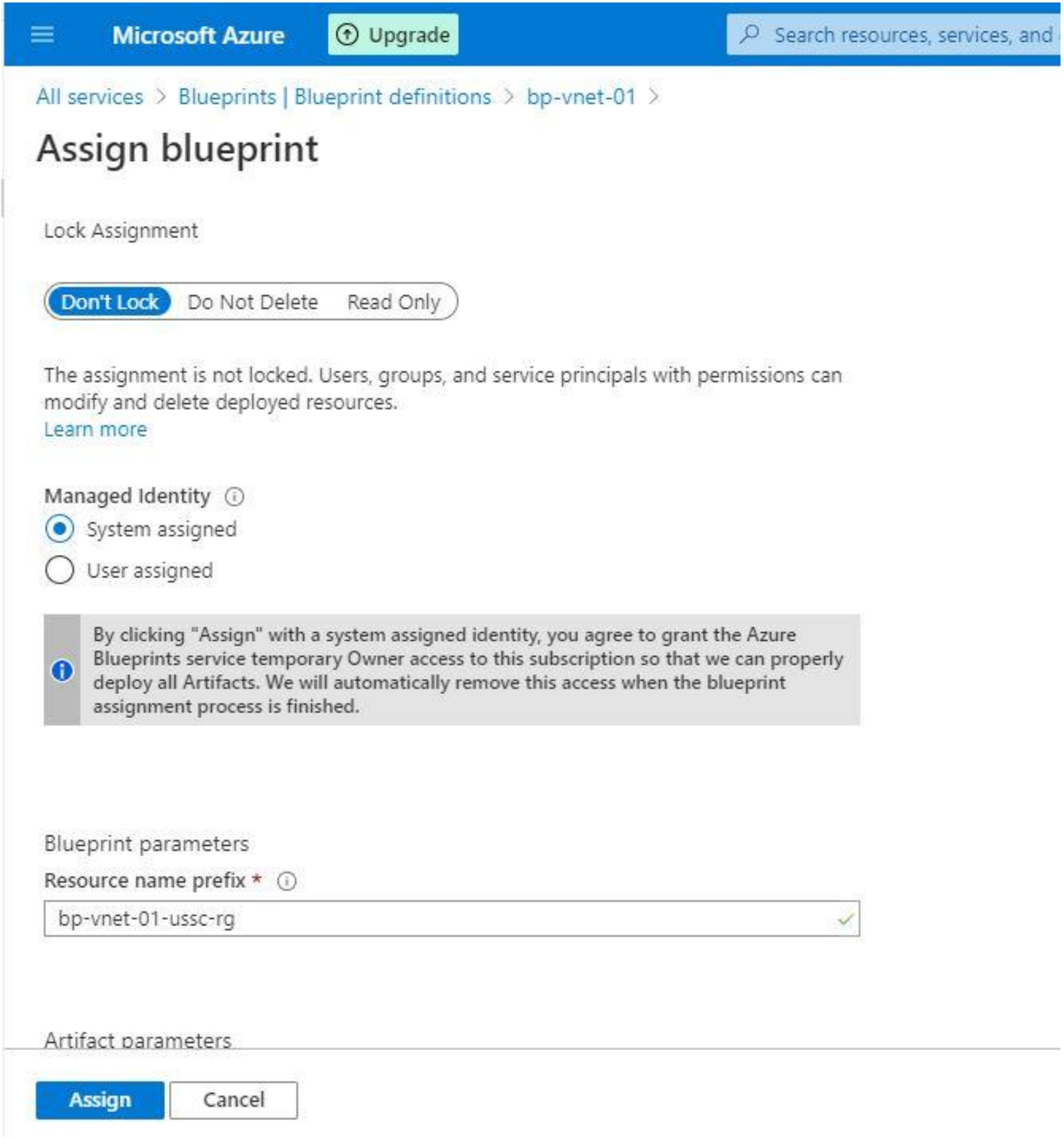
Lock Assignment

● Don't Lock ○ Do Not Delete ○ Read Only

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources.
Learn more

Managed Identity

Figure 15 – Specifying RG (Resource Group)



Microsoft Azure
Upgrade
Search resources, services, and
All services > Blueprints | Blueprint definitions > bp-vnet-01 >

Assign blueprint

Lock Assignment

● Don't Lock ○ Do Not Delete ○ Read Only

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources.
Learn more

Managed Identity

● System assigned

○ User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all Artifacts. We will automatically remove this access when the blueprint assignment process is finished.

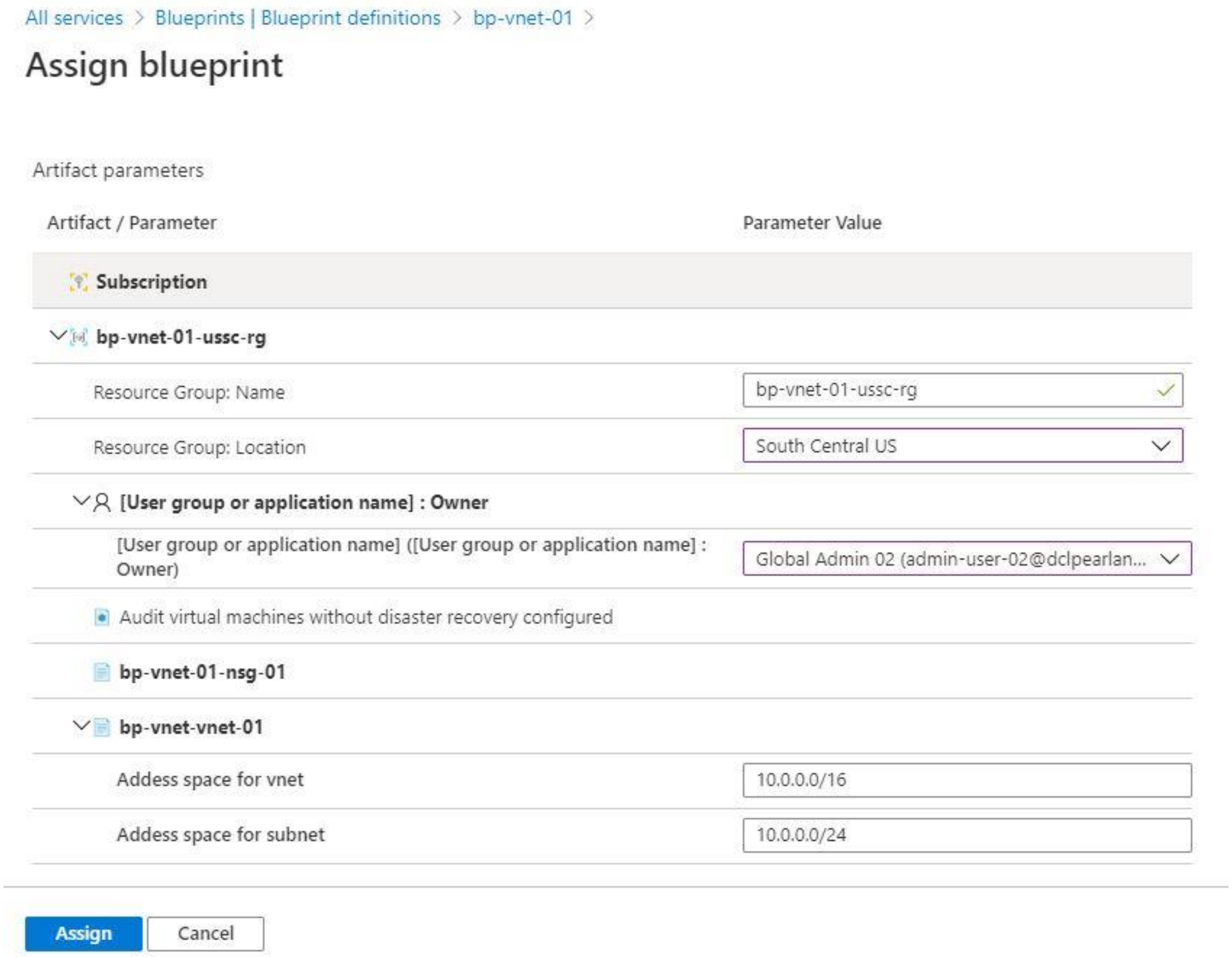
Blueprint parameters

Resource name prefix *

bp-vnet-01-ussc-rg

Artifact parameters

Figure 16 – Populating blueprint parameters



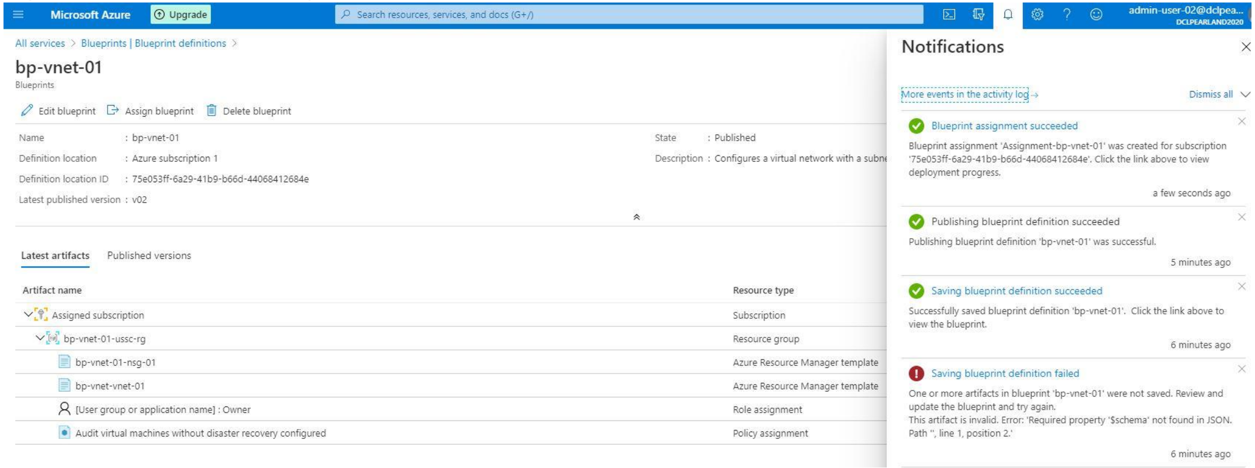
All services > Blueprints | Blueprint definitions > bp-vnet-01 >

Assign blueprint

Artifact parameters

Artifact / Parameter	Parameter Value
Subscription	
bp-vnet-01-ussc-rg	
Resource Group: Name	bp-vnet-01-ussc-rg ✓
Resource Group: Location	South Central US
[User group or application name] : Owner	
[User group or application name] ([User group or application name] : Owner)	Global Admin 02 (admin-user-02@dclpearlan...
Audit virtual machines without disaster recovery configured	
bp-vnet-01-nsg-01	
bp-vnet-vnet-01	
Addess space for vnet	10.0.0.0/16
Addess space for subnet	10.0.0.0/24

Figure 17 – Blueprint assignment succeeded



All services > Blueprints | Blueprint definitions >

bp-vnet-01

Blueprints

Name : bp-vnet-01

Definition location : Azure subscription 1

Definition location ID : 75e053ff-6a29-41b9-b66d-44068412684e

Latest published version : v02

State : Published

Description : Configures a virtual network with a subne

Artifact name	Resource type
Assigned subscription	Subscription
bp-vnet-01-ussc-rg	Resource group
bp-vnet-01-nsg-01	Azure Resource Manager template
bp-vnet-vnet-01	Azure Resource Manager template
[User group or application name] : Owner	Role assignment
Audit virtual machines without disaster recovery configured	Policy assignment

Notifications

Blueprint assignment succeeded

Blueprint assignment 'Assignment-bp-vnet-01' was created for subscription '75e053ff-6a29-41b9-b66d-44068412684e'. Click the link above to view deployment progress.

a few seconds ago

Publishing blueprint definition succeeded

Publishing blueprint definition 'bp-vnet-01' was successful.

5 minutes ago

Saving blueprint definition succeeded

Successfully saved blueprint definition 'bp-vnet-01'. Click the link above to view the blueprint.

6 minutes ago

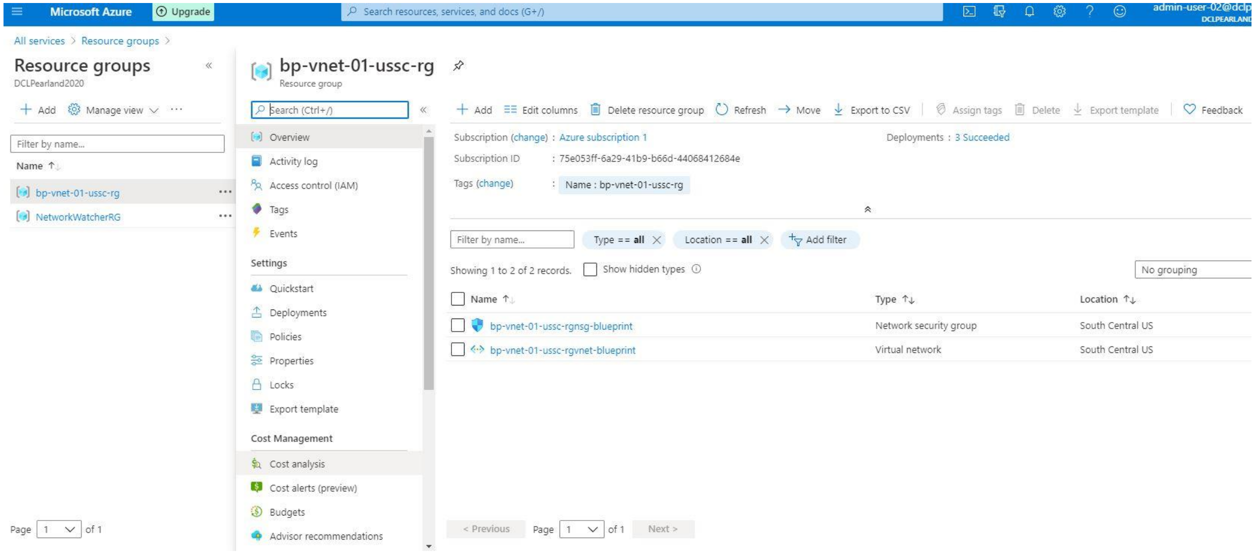
Saving blueprint definition failed

One or more artifacts in blueprint 'bp-vnet-01' were not saved. Review and update the blueprint and try again.
This artifact is invalid. Error: 'Required property '$schema' not found in JSON. Path '', line 1, position 2.'

6 minutes ago

Checking resources created by blueprint

Figure 18 – VNET and NSG created according to the blueprint



Subscription (change) : Azure subscription 1

Subscription ID : 75e053ff-6a29-41b9-b66d-44068412684e

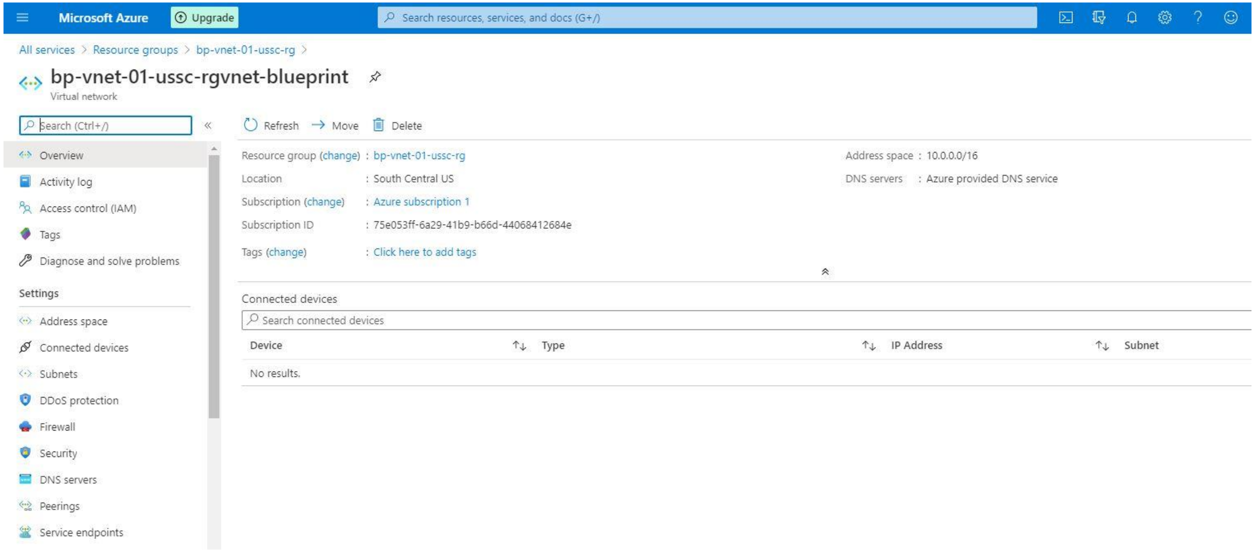
Tags (change) : Name : bp-vnet-01-ussc-rg

Deployments : 3 Succeeded

Showing 1 to 2 of 2 records.

Name ↑↓	Type ↑↓	Location ↑↓
bp-vnet-01-ussc-rgnsg-blueprint	Network security group	South Central US
bp-vnet-01-ussc-rgvnet-blueprint	Virtual network	South Central US

Figure 19 – VNET details



Resource group (change) : bp-vnet-01-ussc-rg

Location : South Central US

Subscription (change) : Azure subscription 1

Subscription ID : 75e053ff-6a29-41b9-b66d-44068412684e

Tags (change) : Click here to add tags

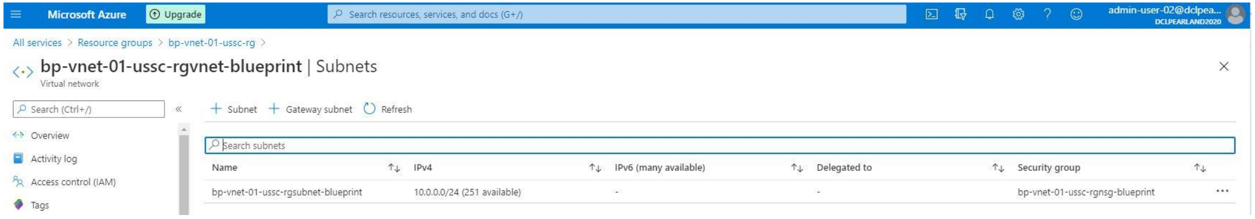
Address space : 10.0.0.0/16

DNS servers : Azure provided DNS service

Connected devices

Device ↑↓	Type ↑↓	IP Address ↑↓	Subnet
No results.			

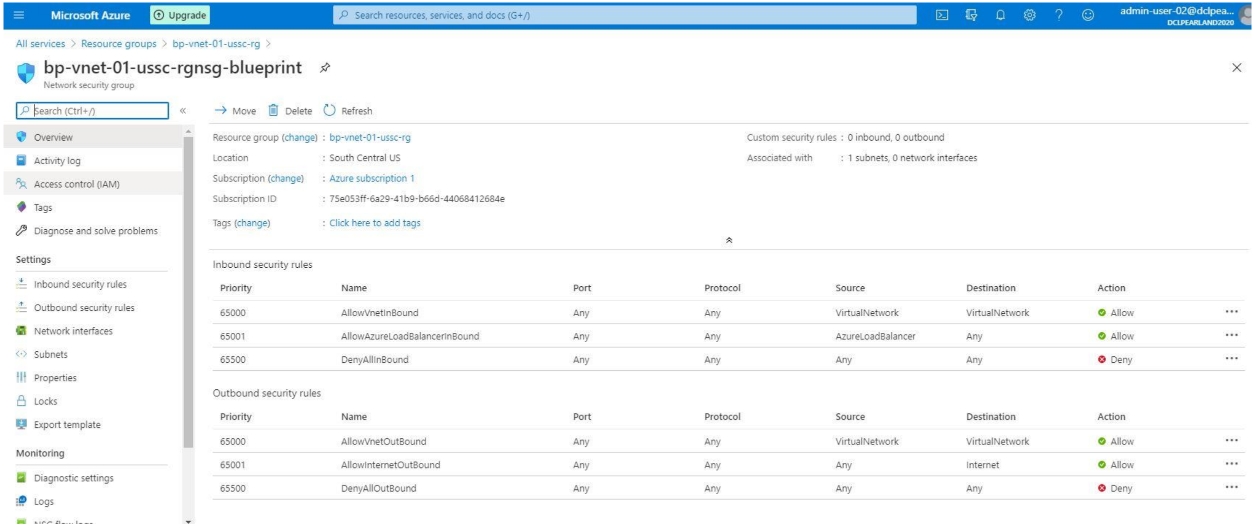
Figure 20 – Subnet details



bp-vnet-01-ussc-rgvnet-blueprint | Subnets
Virtual network

Name	IPv4	IPv6 (many available)	Delegated to	Security group
bp-vnet-01-ussc-rgsubnet-blueprint	10.0.0.0/24 (251 available)	-	-	bp-vnet-01-ussc-rgnsg-blueprint

Figure 21 – NSG details



bp-vnet-01-ussc-rgnsg-blueprint
Network security group

Resource group (change) : bp-vnet-01-ussc-rg
Location : South Central US
Subscription (change) : Azure subscription 1
Subscription ID : 75e053ff-6a29-41b9-b66d-44068412684e
Tags (change) : Click here to add tags

Custom security rules : 0 inbound, 0 outbound
Associated with : 1 subnets, 0 network interfaces

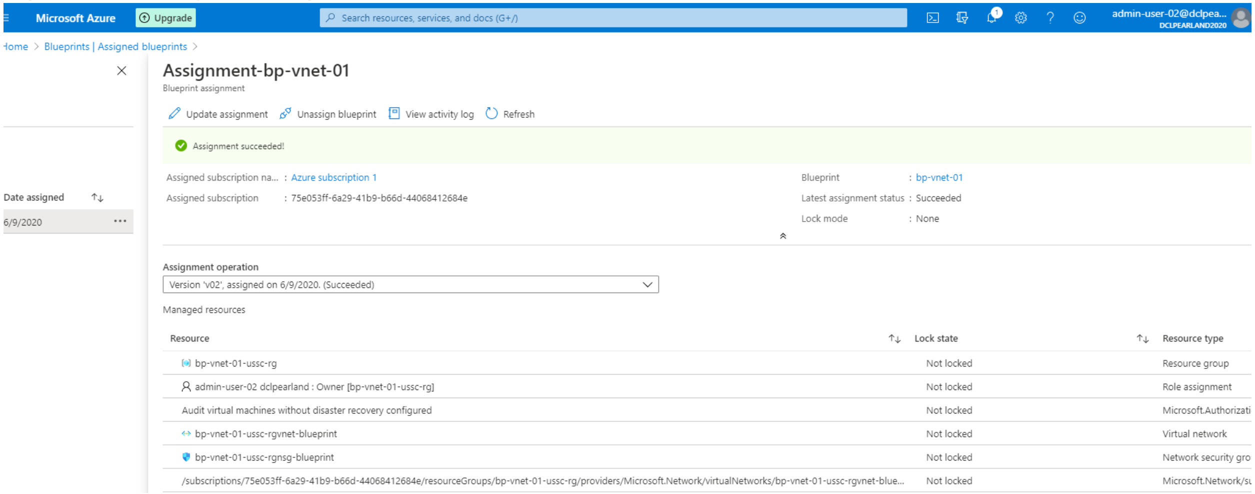
Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Figure 22 – Blueprint assignment details



Date assigned
6/9/2020

Assignment-bp-vnet-01
Blueprint assignment

Assignment succeeded!

Assigned subscription na... : Azure subscription 1
Assigned subscription : 75e053ff-6a29-41b9-b66d-44068412684e

Blueprint : bp-vnet-01
Latest assignment status : Succeeded
Lock mode : None

Assignment operation
Version 'v02', assigned on 6/9/2020. (Succeeded)

Managed resources

Resource	Lock state	Resource type
bp-vnet-01-ussc-rg	Not locked	Resource group
admin-user-02 dclpearland : Owner [bp-vnet-01-ussc-rg]	Not locked	Role assignment
Audit virtual machines without disaster recovery configured	Not locked	Microsoft.Authorizati
bp-vnet-01-ussc-rgvnet-blueprint	Not locked	Virtual network
bp-vnet-01-ussc-rgnsg-blueprint	Not locked	Network security gro
/subscriptions/75e053ff-6a29-41b9-b66d-44068412684e/resourceGroups/bp-vnet-01-ussc-rg/providers/Microsoft.Network/virtualNetworks/bp-vnet-01-ussc-rgvnet-blue...	Not locked	Microsoft.Network/su

Azure CLI Blueprint Extension

Blueprints can be created and managed by Azure CLI for automation

To add blueprint extension, install Azure CLI 2.7.0, the current version

```
azdls1admin@ubun1802:~/scripts/azure$ az --version
azure-cli                         2.7.0
…
```

To check if blueprint is among available extensions

```
azdls1admin@ubun1802:~/scripts/azure$ az extension list-available --output table | grep blue
blueprint                    0.1.0      Microsoft Azure Command-Line Tools Blueprint Extension
False      True           False
```

Note: Older version may not have blueprint as an available extension

To add blueprint extension

```
azdls1admin@ubun1802:~/scripts/azure$ az extension add --name blueprint
The installed extension 'blueprint' is experimental and not covered by customer support. Please use
with discretion.
```

To show help with blueprint

```
azdls1admin@ubun1802:~/scripts/azure$ az blueprint -h

Group
    az blueprint : Commands to manage blueprint.
        This command group is experimental and not covered by customer support. Please use with
        discretion.
Subgroups:
    artifact       : Commands to manage blueprint artifact.
    assignment     : Commands to manage blueprint assignment.
    resource-group : Commands to manage blueprint resource group artifact.
    version        : Commands to manage published blueprint versions.

Commands:
    create        : Create a blueprint definition.
    delete        : Delete a blueprint definition.
    import        : Import a blueprint definition and artifacts from a directoy of json files.
    list          : List blueprint definitions.
    publish       : Publish a new version of the blueprint definition with the latest artifacts.
                    Published blueprint definitions are immutable.
    show          : Get a blueprint definition.
    update        : Update a blueprint definition.

For more specific examples, use: az find "az blueprint"

Please let us know how we are doing: https://aka.ms/clihats
```

To list existing blueprints

```
azdls1admin@ubun1802:~/scripts/azure$ az blueprint list
Command group 'blueprint' is experimental and not covered by customer support. Please use with discretion.
[
  {
    "description": "Configures a virtual network with a subnet and an NSG.",
    "displayName": "Basic Networking (VNET)",
    "id": "/subscriptions/75e053ff-6a29-41b9-b66d-44068412684e/providers/Microsoft.Blueprint/blueprints/bp-vnet-01",
    "layout": null,
    "name": "bp-vnet-01",
    "parameters": {
      "[Usergrouporapplicationname]:Owner_RoleAssignmentName": {
        "allowedValues": null,
        "defaultValue": null,
        "description": null,
        "displayName": "[User group or application name] ([User group or application name] : Owner)",
        "strongType": "PrincipalId",
        "type": "array"
      },
      "addressSpaceForSubnet": {
        "allowedValues": [],
        "defaultValue": "10.0.0.0/24",
        "description": null,
        "displayName": "Addess space for subnet",
        "strongType": null,
        "type": "string"
      },
      "addressSpaceForVnet": {
        "allowedValues": [],
        "defaultValue": "10.0.0.0/16",
        "description": null,
        "displayName": "Addess space for vnet",
        "strongType": null,
        "type": "string"
      },
      "resourceNamePrefix": {
        "allowedValues": null,
        "defaultValue": null,
        "description": "Resource group and resource name prefix",
        "displayName": "Resource name prefix",
        "strongType": null,
        "type": "string"
      }
    },
    "resourceGroups": {
      "SingleRG": {
```

```
    "dependsOn": [],
    "description": null,
    "displayName": "bp-vnet-01-ussc-rg",
    "location": null,
    "name": null,
    "strongType": null,
    "tags": {
     "Name": "bp-vnet-01-ussc-rg"
    }
   }
  },
  "status": {
   "lastModified": "2020-06-09T22:44:48.875216+00:00",
   "timeCreated": "2020-06-09T21:51:07+00:00"
  },
  "targetScope": "subscription",
  "type": "Microsoft.Blueprint/blueprints",
  "versions": null
 }
]
awsdls1admin@ubun1802:~/scripts/azure$
```

For more details of how to use Azure CLI blueprint extension, visit with Azure CLI documentation at https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-azurecli

Conclusion

Landing Zone is an environment created using blueprints. Blueprints can be viewed as elevated Azure Resource Manager (ARM) templates. Blueprints can be edited, expanded by having more artifacts or simplified by removing unwanted artifacts. Blueprints can be versioned, used, revised, and re-used in resource provisioning. Blueprints offer a new way of formulating a consistent and standardized environment across tenants and directories that is called Landing Zone.