Service Principal Test Strategy

# Purpose

This document describes strategy, testing components and prerequisites for Service Principal Solution for test cases define in “[Test Matrix.xlsx](https://microsoft.sharepoint.com/:x:/t/WMTCSEEngagement/EaapFgBz0XxMt4gUoMraPcwB-NZv_pJCzQlVhxDKsaqwog?e=ciFwDD)”

# Components

Authorization

* Application ClientID, it requires the following API permissions
  + Application.ReadWrite.All , User.ReadWrite.All, Directory.ReadWrite.All
* Application Secret
* Tenant ID

Azure active directory

* Dedicated Service Principal Objects created for testing with the following naming convention.
  + sp-AzQueueTesting-[1-n]
* Dedicated Users objects created for testing
  + user-AzQueueTesting-[1-n]

Azure services

* Azure Queue

Test Email Domain names

* Test email domain names are configurable and default to
  + microsoft.com, outlook.com, gmail.com, amazon.com, yahoo.com

Test case ruleset

* Currently we have 11 (eleven) test cases, see “[Test Matrix.xlsx](https://microsoft.sharepoint.com/:x:/t/WMTCSEEngagement/EaapFgBz0XxMt4gUoMraPcwB-NZv_pJCzQlVhxDKsaqwog?e=ciFwDD)” for details

# Prerequisites

Even though Queue Testing Tool will create Service Principal and User Objects it is recommended to have them created ahead of time to save some time.

For this testing we are going to use 3 Service Principals and 3 AAD Users per test case listed below.

**Service Principals**

sp-AzQueueTesting-1, sp-AzQueueTesting-2, . . . . . . . , sp-AzQueueTesting-33

**Users**

user-AzQueueTesting-1, user-AzQueueTesting-2, . . . . . . . , user-AzQueueTesting-33

# Test Cases - Function Evaluate

## TC – 1 – Existing SP has valid Owners, valid Notes (AUDIT PASS)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipal** | SP-1 exists in AAD  SP-1.Owners = [UP-1.UserPrincipalName, UP-2.UserPrincipalName]  SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **ObjectTracking** | Empty or no record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | No change |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity |
|  | **Audit** | AUDIT PASS record exists with correlation id of activity. |

## TC – 2 – Existing SP has no Owners, valid Notes, no LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipal** | SP-1 exists in AAD  SP-1.Owners is empty  SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **ObjectTracking** | Empty or no record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | No change |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity |
|  | **Audit** | AUDIT PASS record exists with correlation id of activity. |

## TC – 2.2 – Existing SP has no Owners, valid Notes, LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipal** | SP-1 exists in AAD  SP-1.Owners is empty  SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **ObjectTracking** | Existing record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | No change |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity |
|  | **Audit** | AUDIT PASS record exists with correlation id of activity. |

## TC – 3 – Existing SP has Owners, invalid Notes (invalid emails), LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | SP-1 exists in AAD  SP-1.Owners = [UP-1.UserPrincipalName, UP-2.UserPrincipalName]  SP-1.Notes = user1@yahoo.com;user2@google.com |
|  | **ObjectTracking** | Existing record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | A ServicePrincipalUpdateCommand message for the corresponding correlationId must exist in Update queue |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity |
|  | **Audit** | AUDIT FAIL records exist with correlation id of activity  Fail\_AttributeValidation – Notes |

## TC – 3.2 – Existing SP has Owners, invalid Notes (invalid emails), no LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | SP-1 exists in AAD  SP-1.Owners = [UP-1.UserPrincipalName, UP-2.UserPrincipalName]  SP-1.Notes = user1@yahoo.com;user2@google.com |
|  | **ObjectTracking** | Empty or no record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | A ServicePrincipalUpdateCommand message for the corresponding correlationId must exist in Update queue |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity |
|  | **Audit** | AUDIT FAIL records exist with correlation id of activity  Fail\_AttributeValidation – Notes |

## TC – 4 – Existing SP has no Owners, invalid Notes (invalid emails), LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | SP-1 exists in AAD  SP-1.Owners is blank  SP-1.Notes = user1@yahoo.com;user2@google.com |
|  | **ObjectTracking** | Existing record for SP-1 SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName  SP.Owners is set since it is LKG |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | A ServicePrincipalUpdateCommand message for the corresponding correlationId must exist in Update queue |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity |
|  | **Audit** | AUDIT FAIL records exist with correlation id of activity  Fail\_AttributeValidation – Notes |

## TC – 5 – Existing SP has no Owners, invalid Notes (invalid emails), no LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | SP-1 exists in AAD  SP-1.Owners is blank  SP-1.Notes = user1@yahoo.com;user2@google.com |
|  | **ObjectTracking** | Empty or no record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | No change |
|  | **ObjectTracking** | Empty or no record for SP-1 |
|  | **Audit** | AUDIT FAIL records exist with correlation id of activity  Fail\_AttributeValidation – Notes |

## TC – 6 – Existing SP has Owners, blank Notes, no LKG (AUDIT FAIL)

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | SP-1 exists in AAD  SP-1.Owners = [UP-1.UserPrincipalName, UP-2.UserPrincipalName]  SP-1.Notes is blank |
|  | **ObjectTracking** | Empty or no record for SP-1 |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | A ServicePrincipalUpdateCommand message for the corresponding correlationId must exist in Update queue |
|  | **ObjectTracking** | Record exists for SP-1  LastUpdated is within (tolerance) seconds  CorrelationId = correlation id of activity  SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **Audit** | AUDIT FAIL records exist with correlation id of activity  Fail\_AttributeValidation – Notes |

# Test Cases - Function Discover

# TC – 1 – Full Seed, HTTP command

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | N/A |
|  | **ServicePrincipal** | SP-1 ... SP-*n* exists in AAD. |
|  | **Command Source** | HTTP |
| Outputs | **UserPrincipals** | N/A |
|  | **ServicePrincipals** | A message should be sent to Evaluate queue for every Service Principal discovered |
|  | **Configuration** | LastSeedTime is within (tolerance) seconds.  Updated DeltaLink is not null or empty  RunState is set to “Delta Run” |
|  | **Activity** | CorrelationId = correlation id of activity  LastUpdated is within (tolerance) seconds.  Name set to “Full Discovery.”  Command Source set to “HTTP” |
|  | **Audit** | N/A |

## TC – 1.2 – Deltas, HTTP command, no change since the last Full seed.

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | N/A |
|  | **ServicePrincipal** | SP-1 ... SP-*n* exists in AAD. No changes have been made to any of the Service Principal objects used for testing since the last full seed. |
|  | **Command Source** | HTTP |
| Outputs | **UserPrincipals** | N/A |
|  | **ServicePrincipals** | A message should be sent to Evaluate queue for every Service Principal discovered. For this case no messages should exist in the queue |
|  | **Configuration** | LastDeltaRun is within (tolerance) seconds.  Updated DeltaLink is not null or empty.  RunState is set to “Delta Run” |
|  | **Activity** | CorrelationId = correlation id of activity  LastUpdated is within (tolerance) seconds.  Name set to “Delta Discovery.”  Command Source set to “HTTP” |
|  | **Audit** | N/A |

## TC – 2 – Full Seed, HTTP command, Service Principal removed

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | N/A |
|  | **ServicePrincipal** | SP-1 was removed. |
|  | **Command Source** | HTTP |
| Outputs | **UserPrincipals** | N/A |
|  | **ServicePrincipals** | A message should be sent to Evaluate queue for every Service Principal discovered. For this case no messages should exist in the queue |
|  | **Configuration** | LastSeedTime is within (tolerance) seconds.  Updated DeltaLink is not null or empty  RunState is set to “Delta Run” |
|  | **Activity** | CorrelationId = correlation id of activity  LastUpdated is within (tolerance) seconds.  Name set to “Full Discovery.”  Command Source set to “HTTP” |
|  | **Audit** | Record must exist for the removed SP.  Code = AuditCode.Ignore\_ServicePrincipalDeleted  Attribute = “AdditionalData”  ExistingAttributeValue = “@removed” |

## TC – 3 – Deltas, HTTP command

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | N/A |
|  | **ServicePrincipal** | SP-2 was modified.  e.g. Assign new Owner. |
|  | **Command Source** | HTTP |
| Outputs | **UserPrincipals** | N/A |
|  | **ServicePrincipals** | A message should be sent to Evaluate queue for every Service Principal discovered as part of the delta. |
|  | **Configuration** | LastUpdated is within (tolerance) seconds.  Updated DeltaLink is not null or empty.  RunState is set to “DeltaRun” |
|  | **Activity** | CorrelationId = correlation id of activity  LastUpdated is within (tolerance) seconds.  Name set to “Delta Discovery.”  Command Source set to “HTTP” |
|  | **Audit** | N/A |

# Test Cases - Function Update

## TC –1 (*Evaluate TC – 3 – Existing SP has Owners, invalid Notes (invalid emails), LKG (AUDIT FAIL))*

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | **SP with a precondition and message in the Queue for**  SP-1 exists in AAD  SP-1.Owners = [UP-1.UserPrincipalName, UP-2.UserPrincipalName]  SP-1.Notes = user1@yahoo.com;user2@google.com |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **Audit** | AUDIT CHANGE records exist with correlation id of activity  Change\_ServicePrincipalUpdated - Notes |

## TC – 2 *(Evaluate TC – 4 – Existing SP has no Owners, invalid Notes (invalid emails), LKG (AUDIT FAIL))*

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | **SP with a precondition and message in the Queue for**  SP-1 exists in AAD  SP-1.Owners is blank  SP-1.Notes = user1@yahoo.com;user2@google.com |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **Audit** | AUDIT CHANGE records exist with correlation id of activity  Change\_ServicePrincipalUpdated - Notes |

## TC – 3 *(Evaluate TC – 6 – Existing SP has Owners, blank Notes, no LKG (AUDIT FAIL))*

|  |  |  |
| --- | --- | --- |
| Inputs | **UserPrincipals** | UP-1, UP-2 exist in AAD |
|  | **ServicePrincipals** | **SP with a precondition and message in the Queue for**  SP-1 exists in AAD  SP-1.Owners = [UP-1.UserPrincipalName, UP-2.UserPrincipalName]  SP-1.Notes is blank |
| Outputs | **UserPrincipals** | No change |
|  | **ServicePrincipals** | SP-1.Notes = UP-1.UserPrincipalName;UP-2.UserPrincipalName |
|  | **Audit** | AUDIT CHANGE records exist with correlation id of activity  Change\_ServicePrincipalUpdated - Notes |