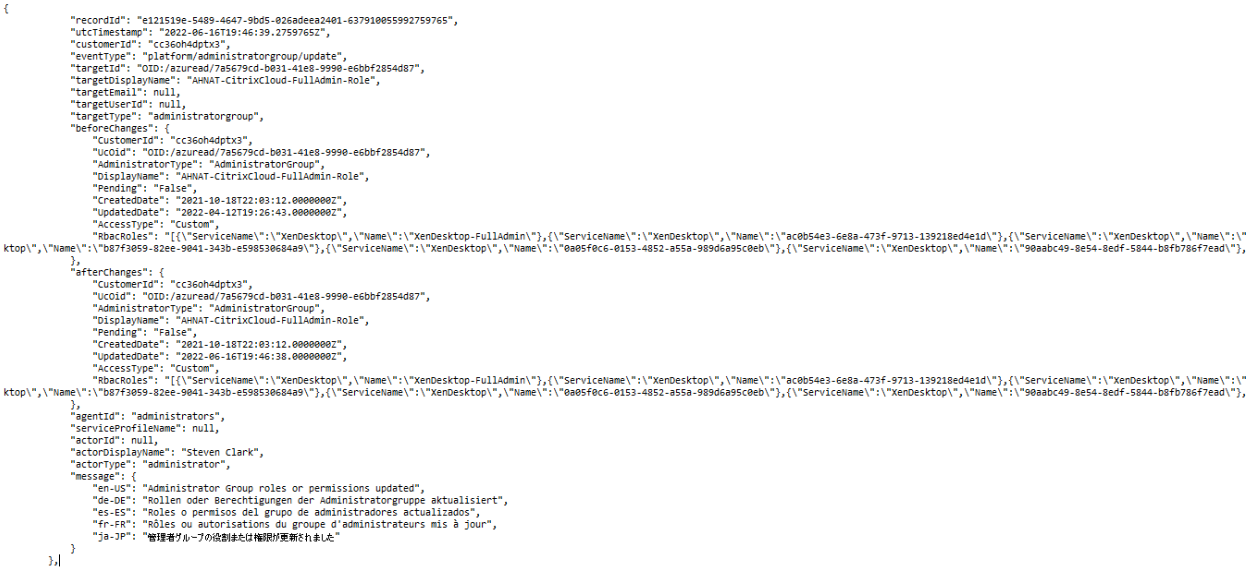
Citrix Audit Logs

Functionality

Collect Citrix Audit logs which helps identify activities performed in the Citrix Cloud environment providing information like what changed, who changed, when it was changed, etc.

API

- API leveraged - https://api-us.cloud.com/systemlog/records
- Reference Documentation - https://developer.cloud.com/citrix-cloud/citrix-cloud---systemlog/docs/overview
- Sample Event -

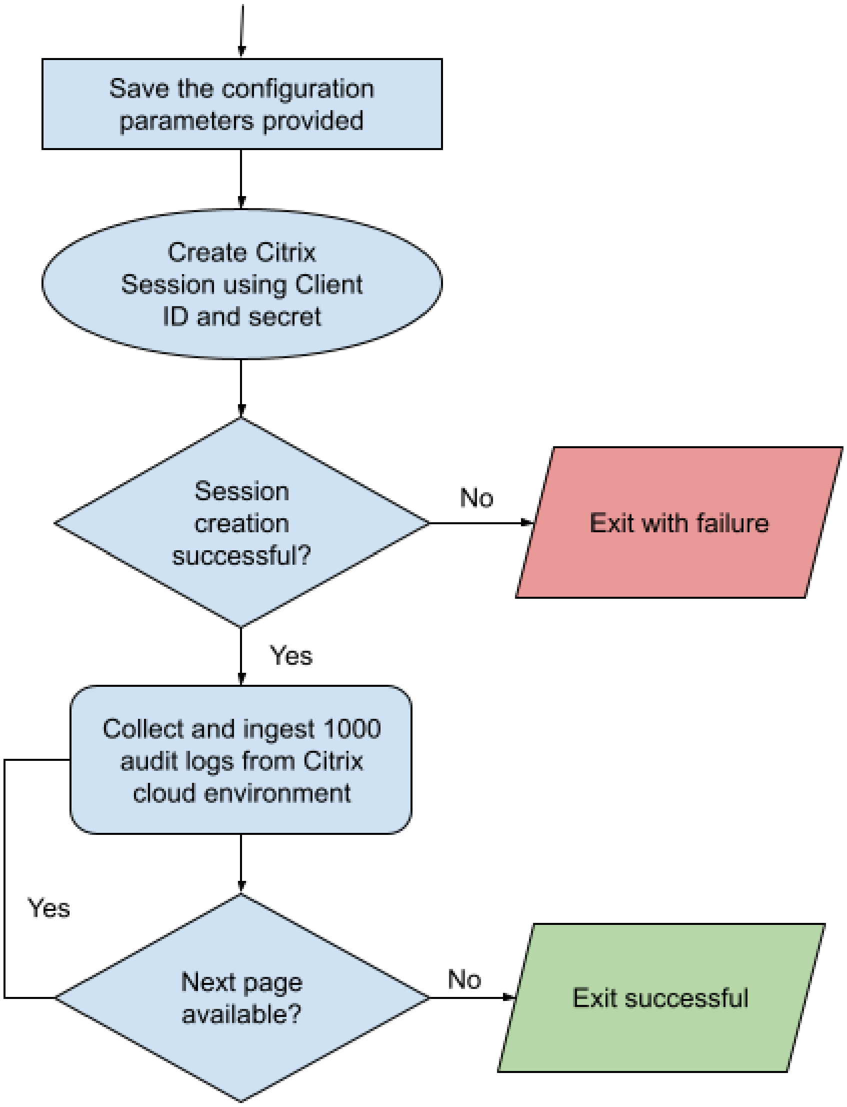


```
{
            "recordId": "e121519e-5489-4647-9bd5-026adeea2401-637910055992759765",
            "utcTimestamp": "2022-06-16T19:46:39.2759765Z",
            "customerId": "cc36oh4dptx3",
            "eventType": "platform/administratorgroup/update",
            "targetId": "OID:/azuread/7a5679cd-b031-41e8-9990-e6bbf2854d87",
            "targetDisplayName": "AHNAT-CitrixCloud-FullAdmin-Role",
            "targetEmail": null,
            "targetUserId": null,
            "targetType": "administratorgroup",
            "beforeChanges": {
                "CustomerId": "cc36oh4dptx3",
                "UcOid": "OID:/azuread/7a5679cd-b031-41e8-9990-e6bbf2854d87",
                "AdministratorType": "AdministratorGroup",
                "DisplayName": "AHNAT-CitrixCloud-FullAdmin-Role",
                "Pending": "False",
                "CreatedDate": "2021-10-18T22:03:12.0000000Z",
                "UpdatedDate": "2022-04-12T19:26:43.0000000Z",
                "AccessType": "Custom",
                "RbacRoles": "[{\"ServiceName\":\"XenDesktop\",\"Name\":\"XenDesktop-FullAdmin\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"ac0b54e3-6e8a-473f-9713-139218ed4e1d\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"
ktop\",\"Name\":\"b87f3059-82ee-9041-343b-e598530684a9\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"0a05f0c6-0153-4852-a55a-989d6a95c0eb\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"90aabc49-8e54-8edf-5844-b8fb786f7ead\"},
            },
            "afterChanges": {
                "CustomerId": "cc36oh4dptx3",
                "UcOid": "OID:/azuread/7a5679cd-b031-41e8-9990-e6bbf2854d87",
                "AdministratorType": "AdministratorGroup",
                "DisplayName": "AHNAT-CitrixCloud-FullAdmin-Role",
                "Pending": "False",
                "CreatedDate": "2021-10-18T22:03:12.0000000Z",
                "UpdatedDate": "2022-06-16T19:46:38.0000000Z",
                "AccessType": "Custom",
                "RbacRoles": "[{\"ServiceName\":\"XenDesktop\",\"Name\":\"XenDesktop-FullAdmin\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"ac0b54e3-6e8a-473f-9713-139218ed4e1d\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"
ktop\",\"Name\":\"b87f3059-82ee-9041-343b-e598530684a9\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"0a05f0c6-0153-4852-a55a-989d6a95c0eb\"},{\"ServiceName\":\"XenDesktop\",\"Name\":\"90aabc49-8e54-8edf-5844-b8fb786f7ead\"},
            },
            "agentId": "administrators",
            "serviceProfileName": null,
            "actorId": null,
            "actorDisplayName": "Steven Clark",
            "actorType": "administrator",
            "message": {
                "en-US": "Administrator Group roles or permissions updated",
                "de-DE": "Rollen oder Berechtigungen der Administratorgruppe aktualisiert",
                "es-ES": "Roles o permisos del grupo de administradores actualizados",
                "fr-FR": "Rôles ou autorisations du groupe d'administrateurs mis à jour",
                "ja-JP": "管理者グループの役割または権限が更新されました"
            }
        },
```

Configuration Parameters

Parameter	Description	Required
Citrix CustomedID	ID of the customer	**Yes**
Citrix URL Domain	Citrix Cloud Endpoint	**Yes**
Citrix Client ID	Citrix API Client ID	**Yes**
Citrix Client Secret	Citrix API Client Secret	**Yes**
Chronicle Function Interval	Interval to consider for collecting the data **Default** - Last 60 mins	**No**

Implementation Approach


Save the configuration parameters provided
Create Citrix Session using Client ID and secret
Session creation successful?
No
Exit with failure
Yes
Collect and ingest 1000 audit logs from Citrix cloud environment
Yes
Next page available?
No
Exit successful

Explanation:

1. Create a Citrix Session by leveraging the URL Domain and the API credentials provided during the configuration.
2. If the session creation is unsuccessful, the script will exit with the respective failure message.
3. If the session creation is successful, the script will commence the data collection considering the interval provided during Configuration.
    - By default, the interval is considered as 60 minutes
    - Start time of data collection will be calculated as (Current time - Interval Provided)

4. In a single API call, the script will collect 1000 records maximum. It will ingest the collected events in Google Chronicle
5. If the API call returns the pagination token for the next set of records, step 4 will be repeated.
6. If the API call does not return the pagination token, the script will exit successfully.