

IT RCSA - Infrastructure

Entity	Apple Bank
Test Name	IT Infrastructure
Test Date	4/9/2021
Process	IT-IFR-P8 Network Privilege Access
Sub-process	Network Privilege Access
Risk # and Description	IT-IFR-R8 - Access to the privilege accounts of the Bank's infrastructure, if unauthorized or inadequately managed, may expose the Bank to privilege misuse and attacks from both internal and external malicious actors
Control # and Description	IT-IFR-C14 Network Privilege Access Privilege access to ABS network and systems is restricted to appropriate individuals with relevant functions.
Level of Risk	High
Control Frequency	As Needed
Process Owner	Debi Gupta
Procedures Performed for Validating Population	Inquiry, Observation, Inspection
SII(s) or Exception(s) Number(s)	Self Reported by Information Security

Test Sample

Control Test Procedures		
Test Step	Test Procedure	
A1	Determine whether there is more than one forest in the AD structure. If yes, determine that external trusts must be authorized. For multiple forest-structure, determine that the administrative control of computers, objects, etc. by users from other forests is restricted or not allowed	Pg. 2, 3
A2	Determine that the AD structure supports the separation between "network admins" (highest admin level) and "network support" (responsible for user credentials, access rights, etc.)	Pg. 4, 5
B1	For global/local GPO, determine that the default policies are defined for password, account lockout, network security - force logoff (when logon hours expire), encryption	Pg. 6, 7
B2	Determine that after 30 days inactivity, the user's remote access will automatically be turned off and account disabled	Pg. 8
B3	Determine that the security/policy settings for privilege accounts are adequate	Pg. 9, 10, 11
B4	For system/generic account, determine that the security/policy settings are adequate	Pg. 12, 13, 14, 15
B5	Determine that the system/generic accounts cannot be used to logon to the network	Pg. 16, 17
C1	For selected shared folders, determine that the settings are appropriate to secure access from unauthorized users	Pg. 18-22



Active Directory Domains and Trusts
APPLEBANK.NY.COM

Name

Type

There are no items to show in this view.

APPLE Bank Single Forest Structure

Trust Level configuration not
necessary in a single forest
structure

A1

APPLEBANK.NY.COM Properties

General Trusts Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive	Properties...	Remove
-------------	------------	------------	---------------	--------

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive	Properties...	Remove
-------------	------------	------------	---------------	--------

New Trust...

OK Cancel Apply Help

Actions

APPLEBANK.NY.COM

More Actions

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-ADForest
>> AC
PS C:\Windows\system32> Get-ADForest

ApplicationPartitions : {DC=ForestDnsZones,DC=APPLEBANK,DC=NY,DC=com, DC=DomainDnsZones,DC=APPLEBANK,DC=NY,DC=com}
CrossForestReferences : {}
DomainNamingMaster    : BR216DC1.APPLEBANK.NY.COM
Domains               : {APPLEBANK.NY.COM}
ForestMode            : Windows2016Forest
GlobalCatalogs       : {br211dc1.APPLEBANK.NY.COM, BR202DC1.APPLEBANK.NY.COM, BR216DC1.APPLEBANK.NY.COM,
                        BR216DC2.APPLEBANK.NY.COM...}
Name                  : APPLEBANK.NY.COM
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=APPLEBANK,DC=NY,DC=com
RootDomain            : APPLEBANK.NY.COM
SchemaMaster          : BR216DC1.APPLEBANK.NY.COM
Sites                 : {BR202, BR211, BR216}
SPNSuffixes           : {}
UPNSuffixes           : {}

PS C:\Windows\system32> _
```

APPLE Bank Single Forest Structure

Trust Level configuration not
necessary in a single forest
structure

A1



Active Directory Users and Computers [BR216DC1.APPLEBANK.NY.COM]

- > Saved Queries
- > APPLEBANK.NY.com
 - > Administrators OU
 - > Branch OU
 - > BSA Contractors OU
 - > Builtin
 - > Computers
 - > Consultants OU
 - > Departments OU
 - > Developmental OU
 - > Distribution Lists
 - > Domain Controllers
 - > Email Service Accounts
 - > ForeignSecurityPrincipals
 - > GROUPS
 - > InactiveComputers
 - > InactiveUsers
 - > LostAndFound
 - > Managed Service Accounts
 - > Member Servers OU
 - > PRINTERS
 - > Program Data
 - > Staging
 - > System
 - > Users
 - > Utility User OU
 - > VMware Horizon OU

Name

- Administrators OU
- Branch OU
- BSA Contractors OU
- Builtin
- Computers
- Consultants OU
- Departments OU
- Developmental OU
- Distribution Lists
- Domain Controllers
- Email Service Accounts
- ForeignSecurityPrincipals
- GROUPS
- InactiveComputers
- InactiveUsers
- Infrastructure
- Keys
- LostAndFound
- Managed Service Accounts
- Member Servers OU
- NTDS Quotas
- PRINTERS
- Program Data
- Staging
- System
- TPM Devices
- Users
- Utility User OU
- VMware Horizon OU

AD structure supports the separation of
"network admins" (highest admin level)

- * Administrators
- * Members of Server groups

from the other business groups, including:

- * Branch
- * BSA Contractors
- * Consultants
- * Departments
- * Developments
- * Utility User
- * VMWare

A2

Type

- Organizational...
- Organizational...
- Organizational...
- builtinDomain
- Container
- Organizational...
- Organizational...
- Organizational...
- Organizational...
- Organizational...
- Container
- Organizational...
- Organizational...
- Unknown
- lostAndFound
- Container
- Organizational...
- Unknown
- Organizational...
- Container
- Organizational...
- Container
- Unknown
- Container
- Organizational...
- Organizational...

Description

- ADMIN
-
-
- Default container for upgraded comp...
-
- Default container for new Windows 2...
-
- Default container for security identifie...
- AD Groups
-
-
- Default container for orphaned objects
- Default container for managed servic...
-
-
- Default location for storage of applica...
-
- Builtin system settings
-
- Default container for upgraded user a...

Service and Delivery Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
Alfi Rosario	APPLEBANK.NY.com/Departments OU/MIS OU...
Avery Lopez	APPLEBANK.NY.com/Departments OU/MIS OU...
Corey Windley	APPLEBANK.NY.com/Departments OU/MIS OU...
Emani Fillyow	APPLEBANK.NY.com/Departments OU/MIS OU...
Emmanuel Oriol	APPLEBANK.NY.com/Departments OU/MIS OU...
Erick Leal	APPLEBANK.NY.com/Departments OU/MIS OU...
Joseph Rinaldi	APPLEBANK.NY.com/Departments OU/MIS OU...
Maria Siegel	APPLEBANK.NY.com/Departments OU/MIS OU...
Obinna Small	APPLEBANK.NY.com/Departments OU/MIS OU...
Rafael Maldo...	APPLEBANK.NY.com/Departments OU/MIS OU...
Reynaldo Fig...	APPLEBANK.NY.com/Departments OU/MIS OU...
Robert Celona	APPLEBANK.NY.com/Departments OU/MIS OU...
Troy Thomas	APPLEBANK.NY.com/Departments OU/MIS OU...
Vinnie Green	APPLEBANK.NY.com/Departments OU/MIS OU...

Add... Remove

OK Cancel Apply Help

Service and Delivery Administrators Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
Alfi Rosario (PA)	APPLEBANK.NY.com/Administrators OU/Users/...
Avery Lopez (...)	APPLEBANK.NY.com/Administrators OU/Users/...
Corey Windle...	APPLEBANK.NY.com/Administrators OU/Users/...
Emani Fillyow ...	APPLEBANK.NY.com/Administrators OU/Users/...
Emmanuel Ori...	APPLEBANK.NY.com/Administrators OU/Users/...
Erick Leal (PA)	APPLEBANK.NY.com/Administrators OU/Users/...
Joseph Rinald...	APPLEBANK.NY.com/Administrators OU/Users/...
Maria Siegel (...)	APPLEBANK.NY.com/Administrators OU/Users/...
Obinna Small ...	APPLEBANK.NY.com/Administrators OU/Users/...
Rafael Maldo...	APPLEBANK.NY.com/Administrators OU/Users/...
Reynaldo Fig...	APPLEBANK.NY.com/Administrators OU/Users/...
Robert Celon...	APPLEBANK.NY.com/Administrators OU/Users/...
Troy Thomas ...	APPLEBANK.NY.com/Administrators OU/Users/...
Vinnie Green (...)	APPLEBANK.NY.com/Administrators OU/Users/...

Add... Remove

OK Cancel Apply Help

Network Infrastructure Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
christine west...	APPLEBANK.NY.com/Departments OU/MIS OU...
Francisco Ortiz	APPLEBANK.NY.com/Departments OU/MIS OU...
Ignacio Sanc...	APPLEBANK.NY.com/Departments OU/MIS OU...
Leon Gilkes	APPLEBANK.NY.com/Departments OU/MIS OU...
Michael Lamp...	APPLEBANK.NY.com/Departments OU/MIS OU...
Rasel Hussain	APPLEBANK.NY.com/Departments OU/MIS OU...

Add... Remove

OK Cancel Apply Help

Network Infrastructure Admins Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
Christine Wes...	APPLEBANK.NY.com/Administrators OU/Users/...
Firepower netf...	APPLEBANK.NY.com/Utility User OU/Users
Francisco Orti...	APPLEBANK.NY.com/Administrators OU/Users/...
Ignacio Sanc...	APPLEBANK.NY.com/Administrators OU/Users/...
Leon Gilkes (...)	APPLEBANK.NY.com/Administrators OU/Users/...
Michael Lamp...	APPLEBANK.NY.com/Administrators OU/Users/...
netfiremonsvc	APPLEBANK.NY.com/Utility User OU/Users
netsolarwindsvc	APPLEBANK.NY.com/Utility User OU/Users
nettenablesvc	APPLEBANK.NY.com/Utility User OU/Users
Rasel Hussai...	APPLEBANK.NY.com/Administrators OU/Users/...
Thycotic Net...	APPLEBANK.NY.com/Utility User OU/Users/Th...

Add... Remove

OK Cancel Apply Help

Server Infrastructure Administrators Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
Aamir Shah (...)	APPLEBANK.NY.com/Administrators OU/Users/...
Christos Spiro...	APPLEBANK.NY.com/Administrators OU/Users/...
Eugene Boyts...	APPLEBANK.NY.com/Administrators OU/Users/...
Neil Franklin (...)	APPLEBANK.NY.com/Administrators OU/Users/...
Nicholas Cree...	APPLEBANK.NY.com/Administrators OU/Users/...
Robert Martin ...	APPLEBANK.NY.com/Administrators OU/Users/...
Stephen Apru...	APPLEBANK.NY.com/Administrators OU/Users/...
Thycotic Serv...	APPLEBANK.NY.com/Administrators OU/Users/...
Uliser Bonilla (...)	APPLEBANK.NY.com/Administrators OU/Users/...
Umar Iqbal (DA)	APPLEBANK.NY.com/Administrators OU/Users/...

Add... Remove

OK Cancel Apply Help

Server Infrastructure Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
Aamir Shah	APPLEBANK.NY.com/Departments OU/MIS OU...
Christos Spiro...	APPLEBANK.NY.com/Departments OU/MIS OU...
Eugene Boyts...	APPLEBANK.NY.com/Departments OU/MIS OU...
Neil Franklin	APPLEBANK.NY.com/Departments OU/MIS OU...
Nicholas Creer	APPLEBANK.NY.com/Departments OU/MIS OU...
Robert Martin	APPLEBANK.NY.com/Departments OU/MIS OU...
Stephen Apru...	APPLEBANK.NY.com/Departments OU/MIS OU...
Uliser Bonilla	APPLEBANK.NY.com/Departments OU/MIS OU...
Umar Iqbal	APPLEBANK.NY.com/Departments OU/MIS OU...

Add... Remove

OK Cancel Apply Help

A2

Network Infrastructure Group, Server Infrastructure Group and Service and Delivery Group were 3 separate logical groups, each with its own members that belong to their own logical group

desktop.ini

Address

6:12 PM
4/30/2021

Default Domain Policy

Scope Details Settings Delegation Status

Default Domain Policy

Data collected on: 4/29/2021 3:02:26 PM

[show all](#)

General

[show](#)

Computer Configuration (Enabled)

[hide](#)

B1

Policies

[hide](#)

Windows Settings

[hide](#)

Security Settings

[hide](#)

Account Policies/Password Policy

[hide](#)

Policy

Enforce password history

Setting

24 passwords remembered

Maximum password age

180 days

Minimum password age

1 days

Minimum password length

14 characters

Password must meet complexity requirements

Enabled

Store passwords using reversible encryption

Disabled

Account Policies/Account Lockout Policy

[hide](#)

Policy

Account lockout duration

Setting

30 minutes

Account lockout threshold

3 invalid logon attempts

Reset account lockout counter after

30 minutes

Account Policies/Kerberos Policy

[show](#)

Local Policies/Audit Policy

[show](#)

Local Policies/Security Options

[hide](#)

Interactive Logon

[show](#)

Network Access

[show](#)

Network Security

[hide](#)

The default policy is defined for password and account lockout

Default Domain Policy

Data collected on: 4/29/2021 3:02:26 PM

[show all](#)

General

[show](#)

Computer Configuration (Enabled)

[hide](#)

Policies

[hide](#)

Windows Settings

B1

[hide](#)

Security Settings

The default policy is defined for network forced logoff

[hide](#)

Account Policies/Password Policy

[show](#)

Account Policies/Account Lockout Policy

[show](#)

Account Policies/Kerberos Policy

[show](#)

Local Policies/Audit Policy

[show](#)

Local Policies/Security Options

[hide](#)

Interactive Logon

[show](#)

Network Access

[show](#)

Network Security

[hide](#)

Policy

Setting

Network security: Do not store LAN Manager hash value on next password change

Enabled

Network security: Force logoff when logon hours expire

Enabled

User Account Control

[show](#)

Other

[show](#)

Event Log

[show](#)

Public Key Policies/Encrypting File System

[show](#)

Advanced Audit Configuration

[show](#)

Administrative Templates

[show](#)

Task Scheduler (Local)

Task Scheduler Library

Microsoft

Symantec Endpoint Protection

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
DCDIAG Report	Ready	At 7:00 AM every day	5/1/2021 7:00:00 AM	4/30/2021 7:00:01 AM	The operation completed successfully. (0x0)	APPLEBK\rmartin_da	12/18/2020
Disable Inactive Computers	Ready	At 5:00 AM every day	5/1/2021 5:00:00 AM	4/30/2021 5:00:01 AM	The operation completed successfully. (0x0)	APPLEBK\rmartin_da	4/2/2021
Manage Inactive Users	Ready	At 5:30 AM every day	5/1/2021 5:30:00 AM	4/30/2021 5:30:01 AM	The operation completed successfully. (0x0)	APPLEBK\rmartin_da	6/1/2021
Reboot	Ready	At 10:00 PM on 12/18/2020		12/18/2020 10:51:49 PM	The operation completed successfully. (0x0)	APPLEBK\rmartin_da	1/2/2021

General

Triggers

Actions

Conditions

Settings

History

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	powershell -File "C:\SCRIPT\AD Inactive Users.ps1"

Task Scheduler Library

Create Basic Task...

Create Task...

Import Task...

Display All Running Tasks

Disable All Tasks History

New Folder...

View

Refresh

Help

Selected Item

Run

End

Disable

Export...

Properties

Delete

Help

Daily job to execute the task (Powershell script) to ensure that after 30 days inactivity, the user's remote access will automatically be turned off and account disabled

B2

Task (Powershell script) to ensure that after 30 days inactivity, the user's remote access will automatically be turned off and account disabled

B2

11:55 AM 4/30/2021



- APPLEBANK.NY.com
 - Administrators OU
 - Groups
 - Users
 - Data Processing
 - Network Infrastructure
 - Project Management
 - Server Infrastructure
 - Aamir Shah (DA)
 - Christos Spiropoulos (DA)
 - Eugene Boytsov (DA)
 - Neil Franklin (DA)
 - Nicholas Creer (DA)
 - Robert Martin (DA)
 - Stephen Apruzzese (DA)
 - Thycotic Server Infrastructure RDP
 - Thycotic ServiceNow Sync
 - Uliser Bonilla (DA)
 - Umar Iqbal (DA)
 - Service and Delivery
 - Branch OU
 - BSA Contractors OU
 - Builtin

Name	Type	Description
Aamir Shah (DA)	User	Administrator
Christos Spiropoulos (DA)	User	Administrator
Eugene Boytsov (DA)	User	Administrator
Neil Franklin (DA)	User	Administrator
Nicholas Creer (DA)	User	Administrator
Robert Martin (DA)	User	Administrator
Stephen Apruzzese (DA)	User	Administrator
Thycotic Server Infrastructure RDP	User	Thycotic RDP access account for Server Infrastructure....
Thycotic ServiceNow Sync	User	Thycotic sync with ServiceNow. 2021-04-14 - Robert ...
Uliser Bonilla (DA)	User	Administrator
Umar Iqbal (DA)	User	Administrator

Server Infrastructure Group containing users with highest privilege access to the ABS network

B3

INC0017644 | Incident | ServiceN

Secret Details - Secret Server

abs.secretservercloud.com/app/#/secret/2697/general

Apps Apple Bank Kace Apple Bank Help D... ADManager Cisco Sectigo Cert Manag...

thycotic

Home

Recent

Shared With Me

Favorites

Inbox

Reports

Secrets

Personal Folders

Aamir Shah

AD Accounts

Data Processing

DBA

EDW

Info Sec

Network Team

Server Team

Data Domain SSH

Local Accounts - Serve...

Local Accounts - Branc...

Local Accounts - VMw...

Server Admins

Admin

Server Team > Server Admins > Aamir Shah - DA access

General Security Audit Remote Password Changing D Heartbeat Change Password Now Launchers More

Basic Information

Contains general information, such as the secret's template type, the domain, the username and password, and other basic information. Depending on permissions, you may not be able to see or edit these fields.

Secret Name *

Aamir Shah - DA access

Edit

Secret Template

Server Team - AD Template

Edit

Domain *

applebank.ny.com

Edit

Username *

aashahda

Edit

Password *

***** Show

Edit

Url

Edit

Url

Edit

Url

Edit

Note

Edit

Aamir Shah - DA access

Domain

applebank.ny.com

Username

aashahda

Password

***** Show

Launchers

RDP Launcher

Web Password Filler

Powershell Launcher

AD Users and Computers

Print Management

PuTTY Launcher

SQL Manager

DNS Manager

AD Users and Computers (CMD)

Privilege accounts are managed through 'Thycotic Secret Server'. The Secret Server ("SS") is a privileged access management (PAM) system that manages who can access what, when, and under whose authority. SS removes vulnerabilities, such as weak passwords or stale user accounts, while discovering the potentially new weaknesses. SS automatically rotates the accounts password in order to further harden the access.

B3

List of applications that this privilege account can access

Access template for a member of the server team

Address

1:47 PM 4/30/2021


```
PS C:\WINDOWS\system32> get-aduser -id aashahda -Properties PasswordExpired, PasswordLastSet, PasswordNeverExpires, PasswordNotRequired, lockoutTime, KerberosEncryptionType
```

```
DistinguishedName      : CN=Aamir Shah (DA),OU=Server Infrastructure,OU=Users,OU=Administrators
                        : OU,DC=APPLEBANK,DC=NY,DC=com
Enabled                 : True
GivenName               : Aamir
KerberosEncryptionType : {}
lockoutTime             : 0
Name                   : Aamir Shah (DA)
ObjectClass             : user
ObjectGUID              : ee09668b-b7a9-4bab-ae7d-7d046277f7f2
PasswordExpired         : False
PasswordLastSet         : 4/25/2021 2:01:00 AM
PasswordNeverExpires    : False
PasswordNotRequired     : False
SamAccountName          : aashahda
SID                    : S-1-5-21-343818398-1336601894-725345543-159675
Surname                 : Shah
UserPrincipalName       : aashahda@APPLEBANK.NY.COM
```

B3

Security setting for privilege access account. This template applies to all privilege accounts.

B3

Password is required and needs be renewed.

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell <https://aka.ms/powershell>

Security setting for generic access account "AD Audit"

B4

```
PS C:\WINDOWS\system32> get-aduser -id adaudit -Properties PasswordExpired, PasswordLastSet, PasswordNeverExpires, PasswordNotRequired, lockoutTime, KerberosEncryptionType
```

```
DistinguishedName      : CN=AD Audit,OU=Users,OU=Utility User OU,DC=APPLEBANK,DC=NY,DC=com
Enabled                : True
GivenName              : AD
KerberosEncryptionType : {}
lockoutTime            : 0
Name                   : AD Audit
ObjectClass            : user
ObjectGUID             : 10647d9e-0054-4e44-bcde-a84f50b56f14
PasswordExpired        : False
PasswordLastSet        : 4/22/2021 3:17:27 PM
PasswordNeverExpires   : True
PasswordNotRequired    : False
SamAccountName         : adaudit
SID                   : S-1-5-21-343818398-1336601894-725345543-127353
Surname               : Audit
UserPrincipalName      : adaudit@APPLEBANK.NY.COM
```

B4

Password is required but needs not be renewed.

PS C:\WINDOWS\system32>

Surname : Audit
UserPrincipalName : adaudit@APPLEBANK.NY.COM

Security setting for generic access account "AD Audit"

B4

PS C:\WINDOWS\system32> get-aduser -id thyadmin -Properties PasswordExpired, PasswordLastSet, PasswordNeverExpires, PasswordNotRequired, lockoutTime, KerberosEncryptionType

DistinguishedName : CN=Thycotic Admin,OU=Thycotic,OU=Users,OU=Utility User OU,DC=APPLEBANK,DC=NY,DC=com
Enabled : True
GivenName : Thycotic
KerberosEncryptionType : {}
lockoutTime : 0

Name : Thycotic Admin

ObjectClass : user
ObjectGUID : 0be34ead-3d90-4727-bc17-2546a27b0b6a
PasswordExpired : False
PasswordLastSet : 4/21/2021 9:17:22 AM

B4

PasswordNeverExpires : True
PasswordNotRequired : False

Password is required but needs not be renewed.

SamAccountName : thyadmin
SID : S-1-5-21-343818398-1336601894-725345543-155527
Surname : Admin
UserPrincipalName : thyadmin@APPLEBANK.NY.COM

PS C:\WINDOWS\system32> thyadmin ^C

PS C:\WINDOWS\system32>

```
PS C:\WINDOWS\system32> get-aduser -id cmdbdcwminysvc -Properties PasswordExpired, PasswordLastSet, PasswordNeverExpires, PasswordNotRequired, lockoutTime, KerberosEncryptionType
```

```
DistinguishedName      : CN=CMDB Domain Controller,OU=ServiceNow,OU=Users,OU=Utility User OU,DC=APPLEBANK,DC=NY,DC=com
Enabled                : True
GivenName              : CMDB
KerberosEncryptionType : {}
Name                   : CMDB Domain Controller
ObjectClass            : user
ObjectGUID             : 43de6aab-24a0-4487-943b-f2230c1a2669
PasswordExpired        : False
PasswordLastSet        : 3/9/2021 10:46:53 AM
PasswordNeverExpires   : True
PasswordNotRequired    : False
SamAccountName         : cmdbdcwminysvc
SID                    : S-1-5-21-343818398-1336601894-725345543-160272
Surname                : Domain Controller
UserPrincipalName      : cmdbdcwminysvc@APPLEBANK.NY.COM
```

Security setting for generic access account "CMDB"

B4

Password is required but needs not be renewed.

```
PS C:\WINDOWS\system32>
```



```
PS C:\WINDOWS\system32> get-aduser -id veeambk -Properties PasswordExpired, PasswordLastSet, PasswordNeverExpires, PasswordNotRequired, lockoutTime, KerberosEncryptionType
```

B4

```
DistinguishedName      : CN=VeeamBK,OU=Users,OU=Utility User OU,DC=APPLEBANK,DC=NY,DC=com
Enabled                : True
GivenName              : VeeamBK
KerberosEncryptionType : {None}
lockoutTime            : 0
Name                   : VeeamBK
ObjectClass            : user
ObjectGUID             : 83a58c72-75a9-4fd6-81fc-15dd55ad87d9
PasswordExpired        : False
PasswordLastSet        : 3/26/2021 1:34:48 PM
PasswordNeverExpires   : True
PasswordNotRequired    : False
SamAccountName         : veeambk
SID                   : S-1-5-21-343818398-1336601894-725345543-158719
Surname               :
UserPrincipalName      : veeambk@APPLEBANK.NY.COM
```

Security setting for generic access account "VeeamBK"

B4

Password is required but needs not be renewed.

```
PS C:\WINDOWS\system32>
```

Service Account Restrictions

Data collected on: 4/30/2021 12:08:58 PM

[show all](#)

General

[hide](#)

Details

[show](#)

Links

[show](#)

Security Filtering

[show](#)

Delegation

[show](#)

Computer Configuration (Enabled)

B5

[hide](#)

Service accounts cannot be used to log on locally



Policies

[hide](#)

Windows Settings

[hide](#)

Security Settings

[hide](#)

Local Policies/User Rights Assignment

[hide](#)

Policy

Setting

Deny log on locally

BUILTIN\Guests, APPLEBK\Service Users

Deny log on through Terminal Services

BUILTIN\Guests, APPLEBK\Service Users

User Configuration (Enabled)

[hide](#)

No settings defined.



General Members Member Of Managed By Object Security



Service Users

Group name (pre-Windows 2000): Service Users

Description: Security Group used for Service Account Restrictions GI

E-mail:

Group scope

- ☐ Domain local
☒ Global
☐ Universal

Group type

- ☒ Security
☐ Distribution

Notes:

B5

Service accounts cannot be used to log on locally (Local domain is disabled)

OK

Cancel

Apply

Help



130%



12:12 PM
4/30/2021



View basic information about your computer

Windows edition

Windows Server 2016 Standard

© 2016 Microsoft Corporation. All rights reserved.

 Windows Server® 2016

System

Processor: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz 2.19 GHz (4 processors)
Installed memory (RAM): 31.3 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: APPLNET1
Full computer name: APPLNET1.APPLEBANK.NY.com
Computer description:
Domain: APPLEBANK.NY.com

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00377-60000-00000-AA934

Advanced Security Settings for content





Name: D:\applenet\consumer_banking\content

Owner: Administrators (APPLENET1\Administrators) [Change](#)

Permissions Share Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

	Type	Principal	Access	Inherited from	Applies to
	Allow	DepOps_AppleNet (APPLEBK\...	Full control	None	This folder, subfolders and files
	Allow	SYSTEM	Full control	None	This folder, subfolders and files
	Allow	Administrators (APPLENET1\...	Full control	None	This folder, subfolders and files
	Allow	Users (APPLENET1\Users)	Read, write & execute	None	This folder, subfolders and files

C1

Full control access to this folder restricted to IT Admin

Add

Remove

View

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK

Cancel

Apply

View basic information about your computer

Windows edition

Windows Server 2016 Standard

© 2016 Microsoft Corporation. All rights reserved.

Windows Server® 2016

System

Processor: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz 2.19 GHz (4 processors)
Installed memory (RAM): 31.3 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: APPLNET1
Full computer name: APPLNET1.APPLEBANK.NY.com
Computer description:
Domain: APPLEBANK.NY.com

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00377-60000-00000-AA934

Advanced Security Settings for files

Name: D:\applenet\corporategovernance\files

Owner: Administrators (APPLENET1\Administrators) [Change](#)

Permissions

Share

Auditing

Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	D:\applenet\corporate...	This folder, subfolders and files
Allow	CorpGov_AppleNet (APPLEBK...	Modify	D:\applenet\corporate...	This folder, subfolders and files
Allow	Administrators (APPLENET1\...	Full control	D:\applenet\corporate...	This folder, subfolders and files
Allow	Uliser Bonilla (DA) (ubonillada...	Full control	D:\applenet\corporate...	This folder, subfolders and files
Allow	Users (APPLENET1\Users)	Read & execute	D:\applenet\corporate...	This folder, subfolders and files

C1

Full control access to this folder restricted to IT Admin and Uliser Bonilla (IT Admin)

Add

Remove

View

Disable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK

Cancel

Apply

View basic information about your computer

Windows edition

Windows Server 2016 Standard

© 2016 Microsoft Corporation. All rights reserved.

 Windows Server® 2016

System

Processor: Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz 2.40 GHz (4 processors)
Installed memory (RAM): 4.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: BKPSVR01
Full computer name: BKPSVR01.APPLEBANK.NY.com
Computer description: Branch backup server 01
Domain: APPLEBANK.NY.com

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00377-70392-37564-AA107

Advanced Security Settings for Compuflex

Name: C:\Compuflex

Owner: Administrators (BKPSVR01\Administrators) [Change](#)

Permissions Share Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	FBA NAVIGATOR (APPLEBK\F...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (BKPSVR01\Ad...	Full control	None	This folder, subfolders and files

C1 Full control access to this folder restricted to IT Admin

Add Remove View

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

View basic information about your computer

Windows edition

Windows Server 2016 Standard

© 2016 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz 2.19 GHz (8 processors)
Installed memory (RAM): 16.0 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: ALMDBERMSVR
Full computer name: ALMDBERMSVR.APPLEBANK.NY.com
Computer description:
Domain: APPLEBANK.NY.com

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00377-70392-37564-AA647

Windows Server® 2016

Advanced Security Settings for Backup

Name: E:\Backup

Owner: Administrators (ALMDBERMSVR\Administrators) [Change](#)

Permissions

Share

Auditing

Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	ALM Service (almsvc@APPLE...	Modify	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	RiskMgmt (APPLEBK\RiskMg...	Modify	None	This folder, subfolders and files
Allow	ADI_Users (APPLEBK\ADI_Us...	Modify	None	This folder, subfolders and files
Allow	Domain Admins (APPLEBK\D...	Full control	None	This folder, subfolders and files
Allow	Administrators (ALMDBERM...	Full control	None	This folder, subfolders and files
Allow	MSSQL SERVER	Full control	None	This folder, subfolders and files

Add

Remove

View

C1

Full control access to this folder restricted to IT Admin

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK

Cancel

Apply

Control Panel > System and Security > System

Search Control Panel

View basic information about your computer

Windows edition

Windows Server 2016 Standard

© 2016 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Xeon(R) G

Installed memory (RAM): 31.3 GB

System type: 64-bit Operating S

Pen and Touch: No Pen or Touch I

Computer name, domain, and workgroup settings

Computer name: APPLNETDEV

Full computer name: APPLNETDEV.AP

Computer description:

Domain: APPLEBANK.NY.co

Windows activation

Windows is activated [Read the Microsoft Soft](#)

Product ID: 00377-60000-00000-AA934

Advanced Security Settings for files

Name: D:\applenet\policies\files

Owner: Administrators (APPLNETDEV\Administrators) [Change](#)

Permissions | Share | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

	Type	Principal	Access	Inherited from	Applies to
	Allow	ERM_Applenet (APPLEBK\ER...	Modify	None	This folder, subfolders and files
	Allow	Administrators (APPLNETDE...	Full control	None	This folder, subfolders and files
	Allow	SYSTEM	Full control	None	This folder, subfolders and files
	Allow	Everyone	Modify	None	This folder, subfolders and files

C1 Full control access to this folder restricted to IT Admin

[Add](#) [Remove](#) [View](#)

[Enable inheritance](#)

☐ Replace all child object permission entries with inheritable permission entries from this object

[OK](#) [Cancel](#) [Apply](#)