

VDI

Guida alla configurazione del join a dominio AD di una VM

Versione 5.4.0



Sommario

Capitolo 1 Introduzione alla funzione	1
1.1 Scenario applicativo	1
1.2 Teoria dell'implementazione.....	1
1.2.1 Limitare l'accesso degli utenti di dominio	1
1.2.2 Aggiunta alla OU specificata o unirsi al gruppo di gestione locale	2
1.2.3 Aggiungere il dominio e l'accesso automatico al dominio.....	2
1.2.4 Configurazione della macchina virtuale.....	2
Capitolo 2: Processo di configurazione e precauzioni.....	3
2.1 Creazione utente AD	3
2.2 Configurare l'autenticazione LDAP nel VDC	6
2.3 Creare una risorsa e aggiungere la macchina virtuale al dominio.....	14
2.4 Introduzione e configurazione dell'ottimizzazione del dominio AD.....	21
2.4.1 Aggiunta di una VM ad una OU specificata	22
2.4.2 Accesso automatico dell'utente di dominio	23
2.4.3 Associare l'accesso dell'utente di dominio	24
2.4.4 L'utente di dominio si unisce automaticamente al gruppo Administrators locale o Power Users.	25
2.4.5 Altre caratteristiche.....	26
Capitolo 3: Descrizione della registrazione (LOG) dei processi effettuati	28
4.1 Aggiunta VM a domino / aggiunta a OU non riuscito.....	30
4.2 Desktop virtuale aggiunto al dominio ma accesso automatico al dominio non riuscito.....	31
4.3 Errore nell'aggiunta al gruppo di gestione locale	32
4.4 La funzione di associazione è in errore	32
4.5 Errore di accesso automatico	33

Capitolo 1 Introduzione alla funzione

1.1 Scenario applicativo

Questa funzione è applicabile ad un ambiente di Dominio Microsoft AD dove la macchina virtuale necessita essere aggiunta per poter accedere alla rete Intranet del cliente ed essere controllata nel dominio AD. Allo stesso tempo, la configurazione del dominio Active Directory può essere completata insieme al VDC, semplificando il processo di distribuzione del cloud desktop e del dominio AD.

Le seguenti funzioni possono essere implementate:

1. VM aggiunta al dominio. Incluso il tipo di desktop dedicato e ripristinato.
2. Aggiunta della macchina virtuale al dominio AD o all'unità organizzativa specificata. Per impostazione predefinita si unirà all'unità organizzativa Computer, è possibile configurare l'unità organizzativa desiderata.
3. Gli utenti di dominio (Domain Users) accedono automaticamente. Gli utenti di dominio (Domain Users) possono usare VDI SSO per la macchina virtuale.
4. Associare l'accesso per utente di dominio. Solo l'account VDI associato è autorizzato ad accedere alla macchina virtuale, gli altri utenti di dominio (Domain Users) non sono autorizzati ad accedere.
5. Gli utenti di dominio (Domain Users) si uniscono automaticamente al gruppo di amministratori locali o al gruppo Power Users.
6. Gli utenti di dominio legano l'accesso al nome del computer. La configurazione di accesso dell'utente del dominio è legata al nome del computer specificato.
7. Il nome utente del dominio non fa distinzione tra maiuscole e minuscole.

1.2 Teoria dell'implementazione

1.2.1 Limitare l'accesso degli utenti di dominio

1. **VDC:** Aggiungere il plug-in, immettere le informazioni sul dominio da

associare e fornire la configurazione.

2. **Vdagent:** riceve la configurazione, legge le informazioni di associazione pertinenti e scrive le informazioni vincolanti nel Registro di sistema.
3. **Vdsso:** Completa l'inserimento del nome utente e della password, avvia l'operazione di login e determina se l'utente corrente soddisfa o meno le condizioni di accesso. (Windows 7/10 e Windows XP sono due metodi di funzionamento completamente diversi)

1.2.2 Aggiunta alla OU specificata o unirsi al gruppo di gestione locale

1. **VDC:** aggiungi l'interfaccia di configurazione e immetti la configurazione.
2. **Vdagent:** Riceve un messaggio da VDC e scrive nella memoria condivisa.
3. **Vdnetdom:** Legge il messaggio nella memoria condivisa ed esegue l'operazione di accesso automatico.

1.2.3 Aggiungere il dominio e l'accesso automatico al dominio

1. **VDC:** aggiungi un'interfaccia di configurazione e invia operazioni per dominio o di accesso automatico.
2. **Vdagent:** Riceve un messaggio da VDC e scrive nella memoria condivisa.
3. **Vdsso:** Legge il messaggio nella memoria condivisa per l'accesso automatico.

1.2.4 Configurazione della macchina virtuale

1. Associa il dominio e il percorso di archiviazione dell'utente di dominio, il percorso del registro di sistema è:

**KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SfSysPrep\CP
UID**

Campi correlati: **binddomain** (bind domain name), **username** (bound user), **isbindvmuser** (indipendentemente dal fatto che gli utenti siano collegati o meno).

2. Il file di configurazione xml inviato alla macchina virtuale può essere aperto direttamente in:

C:

\Users\ad_uu\AppData\Local\SangforVDI\ShellMsg_01_s1_5963248b.dat

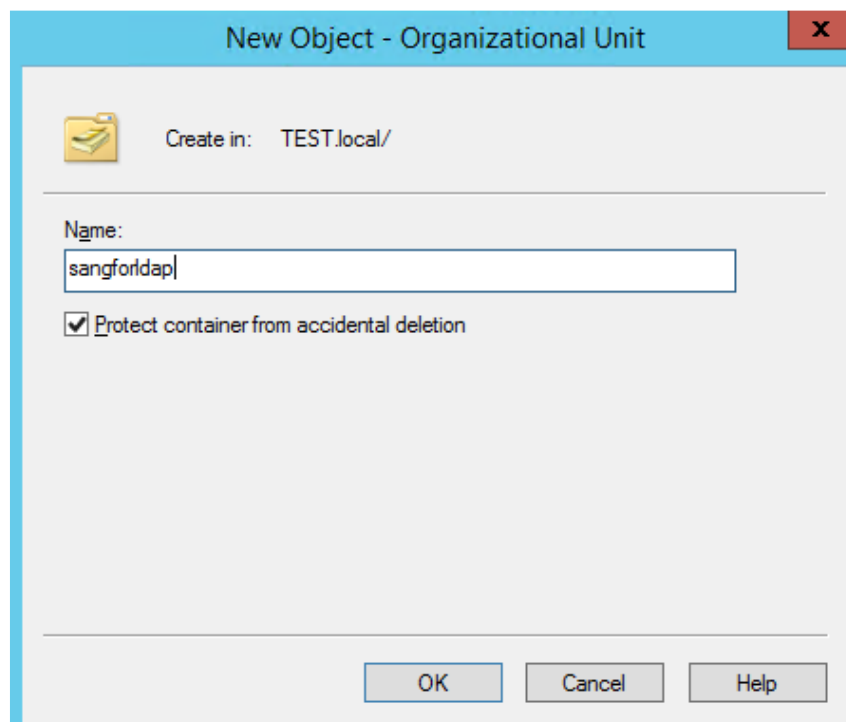
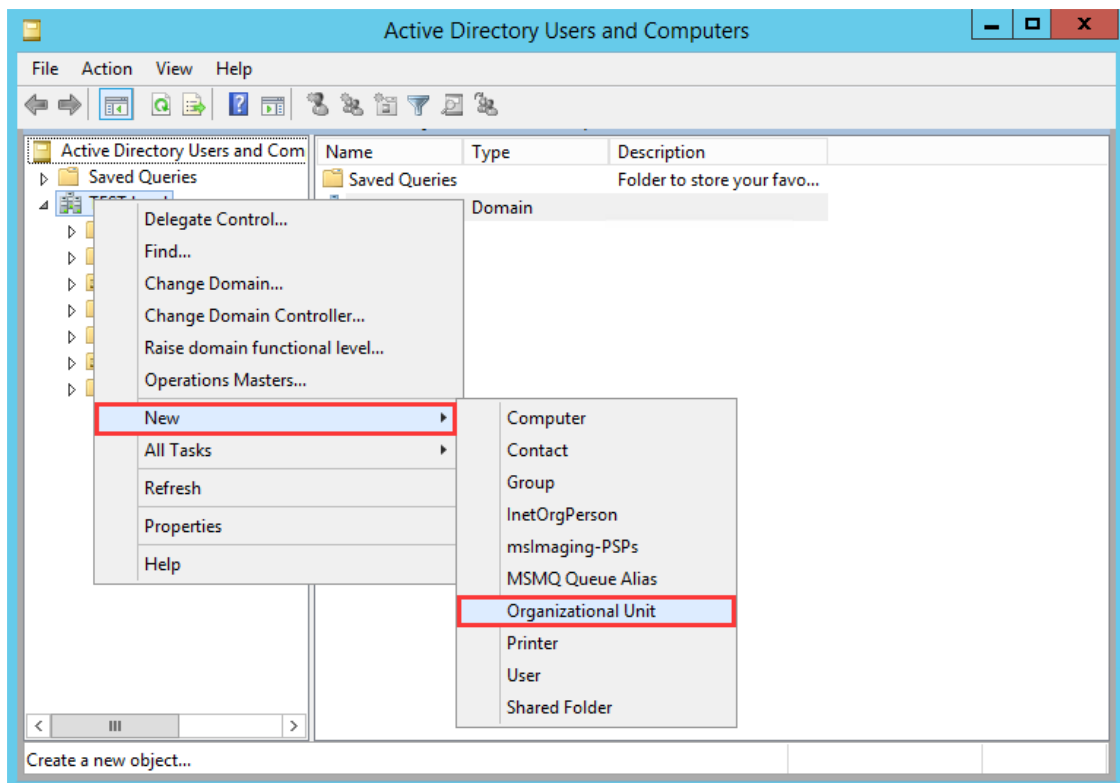
Capitolo 2: Processo di configurazione e precauzioni

Precauzioni:

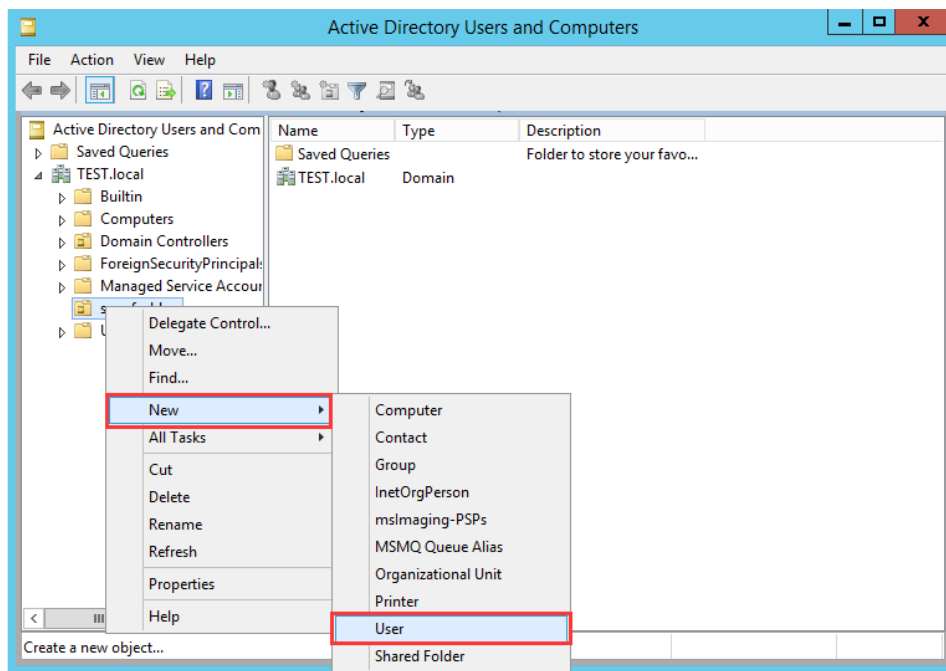
1. Per l'aggiunta di una VM alle funzioni di dominio, il template non deve essere aggiunto al dominio.
2. Non modificare il SID della macchina virtuale creata.

2.1 Creazione utente AD

1. Apri il tool **Utenti e computer di Active Directory**, crea una nuova **unità organizzativa** sotto il dominio come da figura seguente:



2. Creare utenti sotto l'unità organizzativa, creata precedentemente, come da figura seguente:



The 'New Object - User' dialog box is shown, titled 'New Object - User'. The 'Create in:' field is set to 'TEST.local/sangfordap'. The following fields are filled out:

- First name: sangfor
- Last name: user
- Full name: sangfor user
- User login name: sangforuser (with a dropdown menu showing '@TEST.local')
- User login name (pre-Windows 2000): TEST\ sangforuser

Navigation buttons at the bottom: '< Back', 'Next >', and 'Cancel'.

The 'New Object - User' dialog box is shown, titled 'New Object - User'. The 'Create in:' field is set to 'TEST.local/sangfordap'. The following fields are filled out:

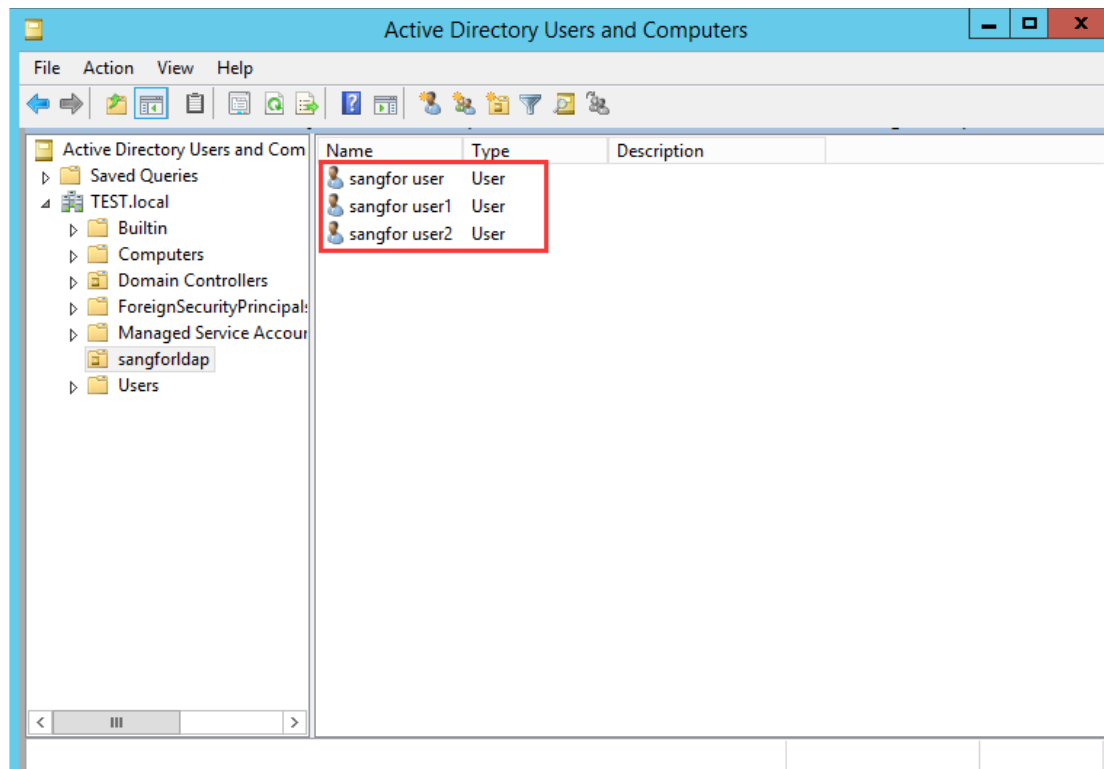
- Password: [Redacted with dots]
- Confirm password: [Redacted with dots]

Below the password fields are four checkboxes:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled

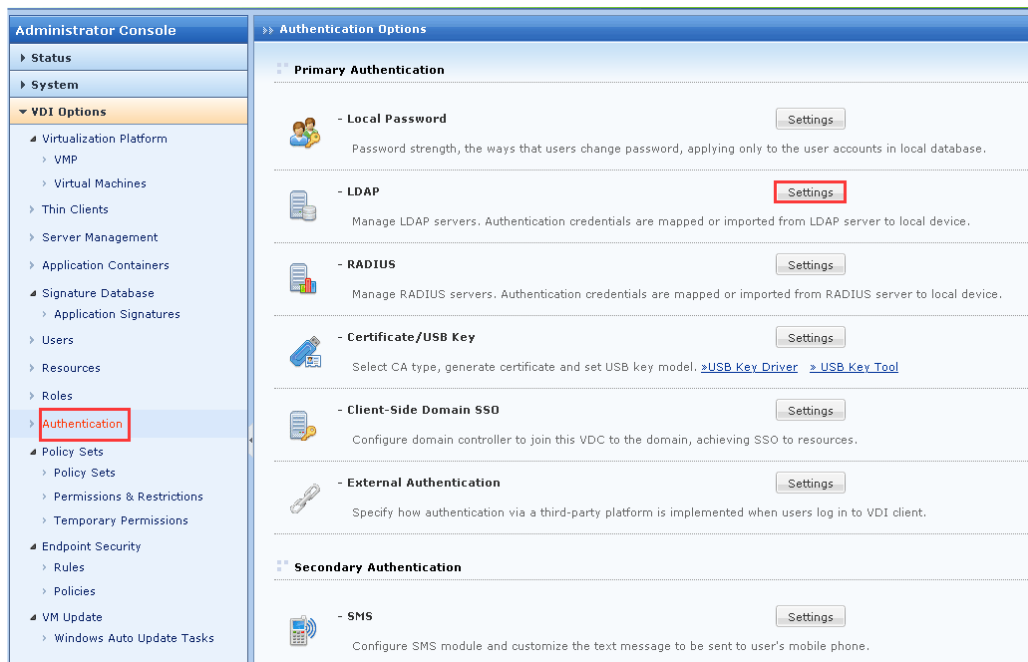
Navigation buttons at the bottom: '< Back', 'Next >', and 'Cancel'.

3. Utilizzare il seguente metodo per creare gli utenti.

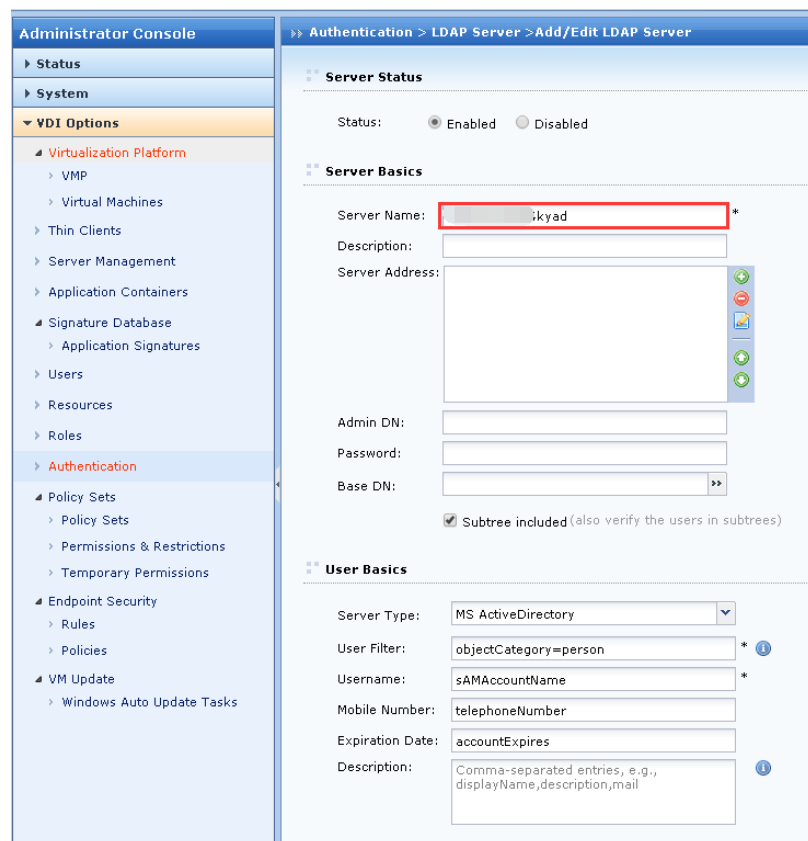


2.2 Configurare l'autenticazione LDAP nel VDC

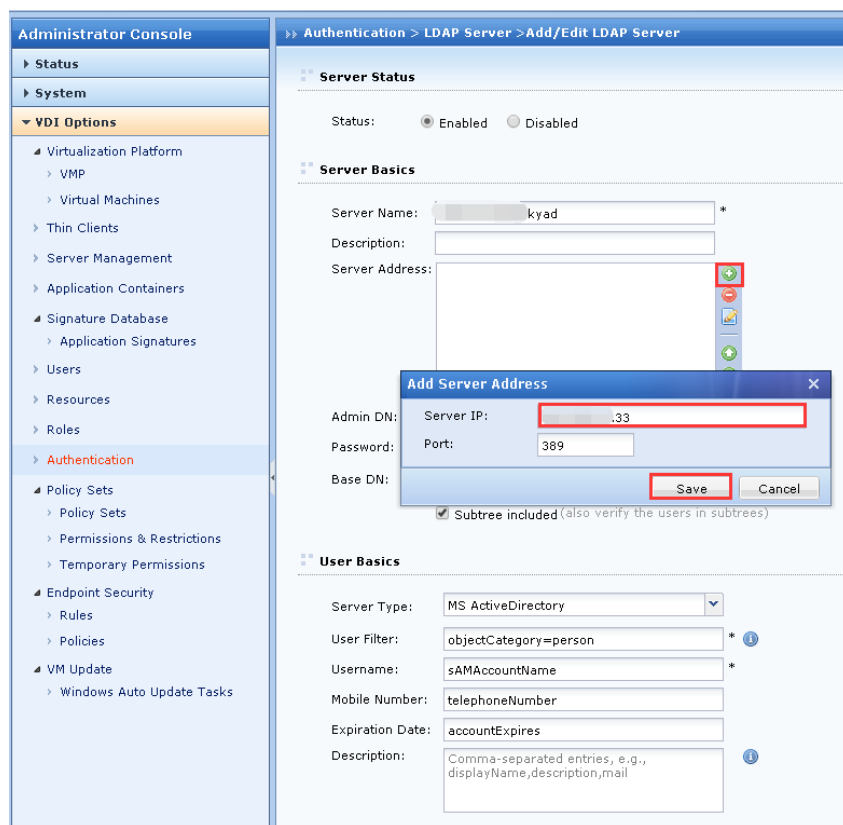
1. Vai a **VDI Options > Authentication**, fai clic sul pulsante **Settings** accanto alle opzioni **LDAP** come nella figura seguente:



2. Fare clic sul pulsante **Nuovo**, quindi immettere il nome del server:



3. Fare clic sul pulsante **verde** accanto alla casella **“Server Address”** per aggiungere l’indirizzo IP del server (la porta predefinita è 389) come indicato di seguito:



4. Inserisci in **“Admin DN”** il nome utente e la password come nella figura seguente:

Administrator Console >> Authentication > LDAP Server > Add/Edit LDAP Server

► Status

► System

▼ VDI Options

- Virtualization Platform
 - VMP
 - Virtual Machines
 - Thin Clients
 - Server Management
 - Application Containers
- Signature Database
 - Application Signatures
- Users
- Resources
- Roles
- Authentication
- Policy Sets
 - Policy Sets
 - Permissions & Restrictions
 - Temporary Permissions
- Endpoint Security
 - Rules
 - Policies
- VM Update
 - Windows Auto Update Tasks

Server Status

Status: ☒ Enabled ☐ Disabled

Server Basics

Server Name: 192.200.19.54kyad *

Description:

Server Address: 192.200.19.33:389

Admin DN: admin@TEST

Password:

Base DN: >>

☒ Subtree included (also verify the users in subtrees)

User Basics

Server Type: MS ActiveDirectory

User Filter: objectCategory=person *

Username: sAMAccountName *

Mobile Number: telephoneNumber

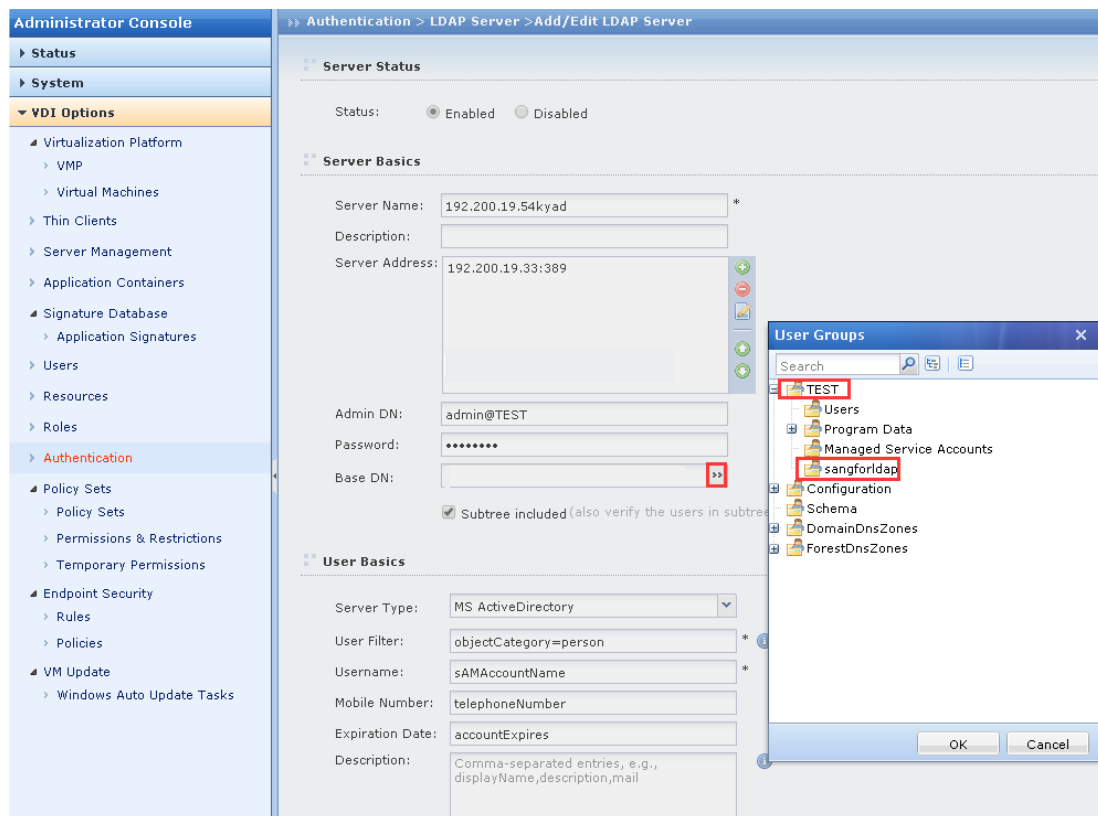
Expiration Date: accountExpires

Description: Comma-separated entries, e.g., displayName,description,mail



Nota: ad esempio, l'account dell'amministratore del server è **admin** e il nome di dominio è **TEST**, quindi nel campo Admin DN inserire **admin@TEST**.

- Fare clic sul pulsante accanto alla casella "**Base DN**", quindi selezionare la struttura organizzativa dell'utente nel dominio e fare clic sul pulsante **Salva** per completare la configurazione come figura seguente:



6. Vai a **VDI options > Users > New > Group** >, inserisci il nome del gruppo. Deselezionare gli attributi **Inherit parent group's attributes**. In **Authentication Setting**, scegliere **External LDAP/RADIUS**, scegliere il metodo di autenticazione che sarà creato nel passo successivo, come da figura seguente:

Edit User Group

Basic Attributes

Name: *

Description:

Added To: >>

Area: >> ⓘ

Max Concurrent Users: (0 indicates no limit)

Status: ☒ Enabled ☐ Disabled

☐ Inherit parent group's attributes

☐ Inherit authentication settings

☐ Inherit policy set

☐ Inherit assigned roles

Authentication Settings

Primary Authentication

☐ Local password

☐ Certificate/USB key

☒ External LDAP/RADIUS ▾

Require: ☒ Both ☐ Either

☐ Enforce its users/subgroups to inherit the authentication settings

Secondary Authentication

☐ Hardware ID

☐ SMS password based

☐ Dynamic token ▾

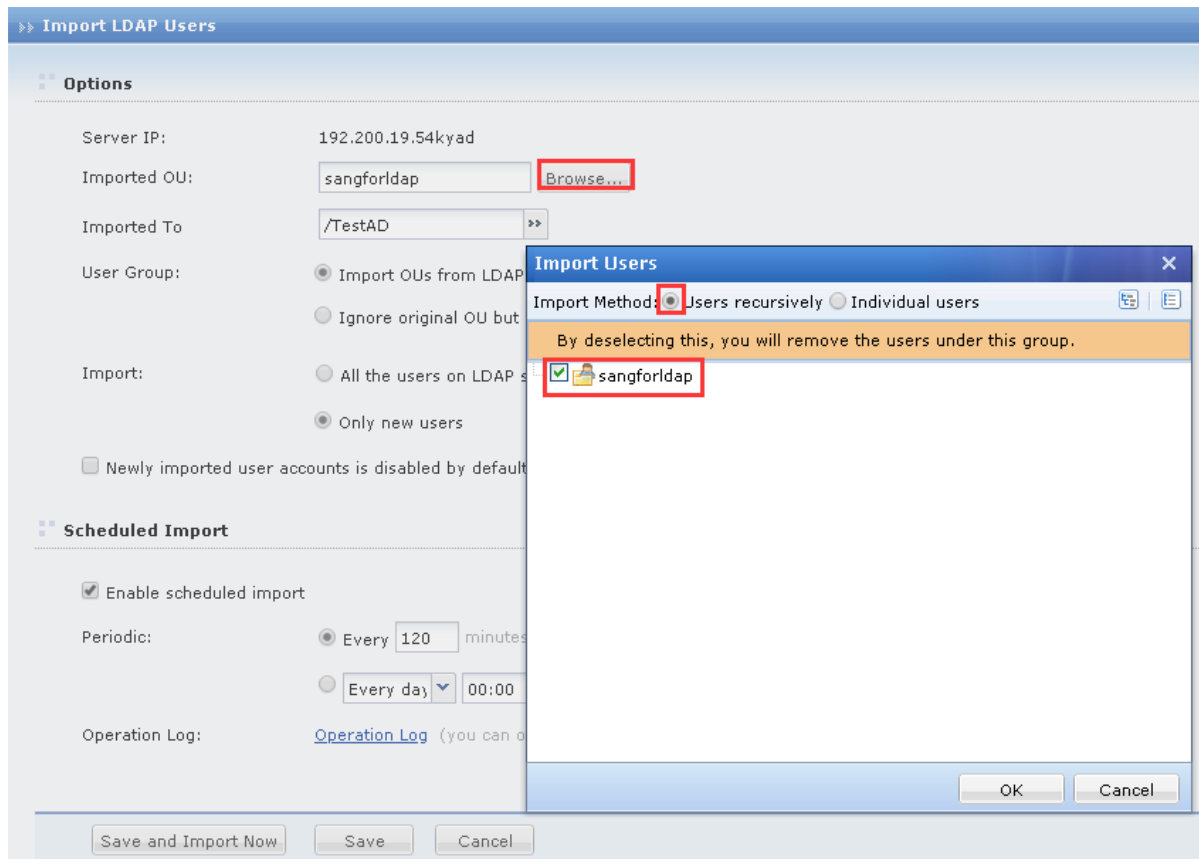
7. Vai su **VDI Options > Authentication**, scegli il metodo di autenticazione creato poco fa e fai clic sul pulsante **Importa utenti** come figura sotto:

LDAP Server

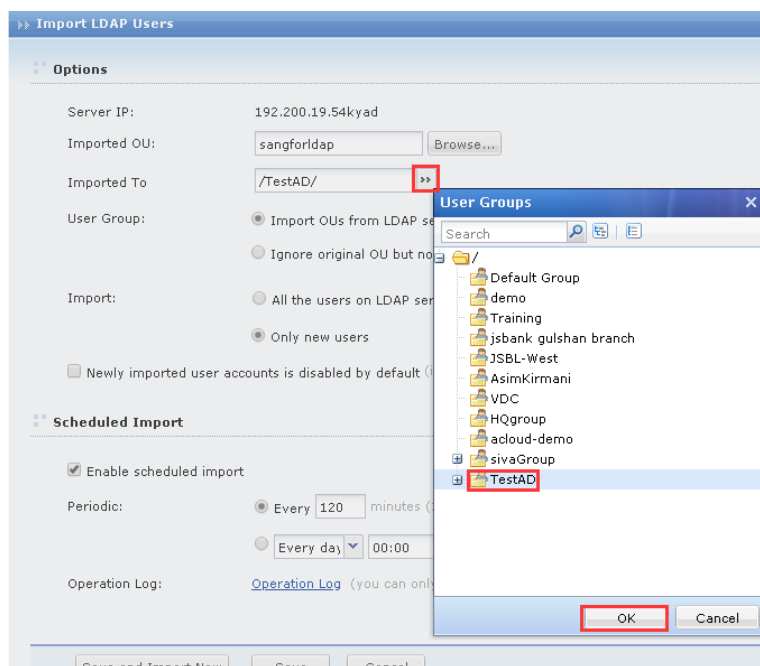
New Delete Edit Import Users

Name	Description	Type	Address	Port
<input type="checkbox"/> Siva		MS ActiveDirectory	192.168.19.209	389
<input checked="" type="checkbox"/> 192.200.19.54kyad		MS ActiveDirectory	192.200.19.33	389
<input type="checkbox"/> jh_test		MS ActiveDirectory	192.200.19.112	389
<input type="checkbox"/> bill		MS ActiveDirectory	192.168.19.219	389
<input type="checkbox"/> 192.168.19.89		MS ActiveDirectory	192.168.19.89	389
<input type="checkbox"/> exam		MS ActiveDirectory	192.168.20.45	389
<input type="checkbox"/> ADServer		MS ActiveDirectory	192.168.20.142	389

8. Fare clic sul pulsante **Sfoglia** accanto alla casella **"Imported OU"**, quindi scegliere **"Users recursively"** e la OU creata precedentemente.



9. Fare clic sul pulsante accanto alla casella **"Imported To"**, per scegliere il gruppo di utenti che è stato creato prima.



10. Le impostazioni di **User Group** e **Import** è possibile modificarle in base ai requisiti richiesti.

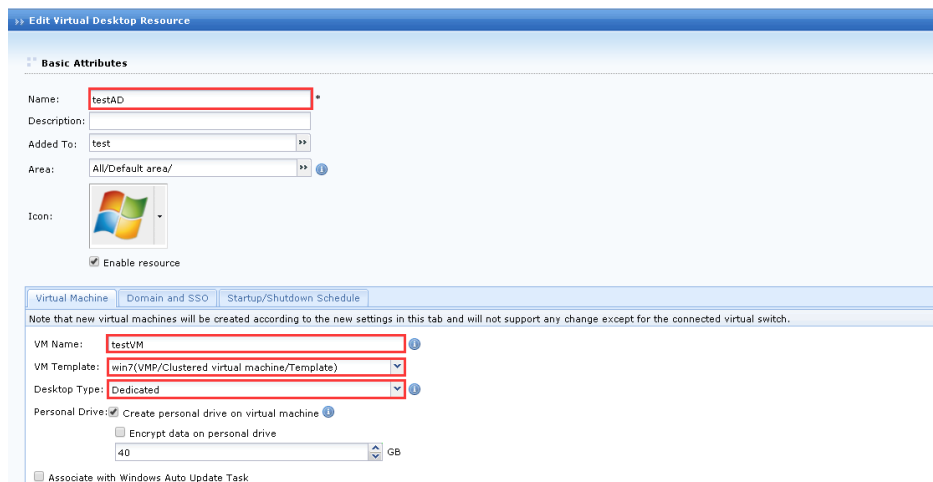
11. Se è richiesta un'importazione pianificata, fare clic sulla casella **Enable schedule**. Le impostazioni possono essere modificate a piacimento in base alle proprie necessità.

12. Fare clic sul pulsante **Save and Import Now**, gli utenti sul dominio si sincronizzeranno con il gruppo utenti. Vai a **VDI Options > Users**, scegli il gruppo di utenti e controlla se gli utenti del dominio sono stati sincronizzati o meno.

Name	Type	Policy Sets	Role	Area	Description	Valid To	Last Login	Mobile Number	Virtual IP	Status
sangforuser	User	Default policy set		Default area		Never expire	Never logged in		Auto assigned	✓
sangforuser1	User	Default policy set	ADtest	Default area		Never expire	2019-08-28 1...		Auto assigned	✓
sangforuser2	User	Default policy set	ADtest	Default area		Never expire	2019-08-28 1...		Auto assigned	✓

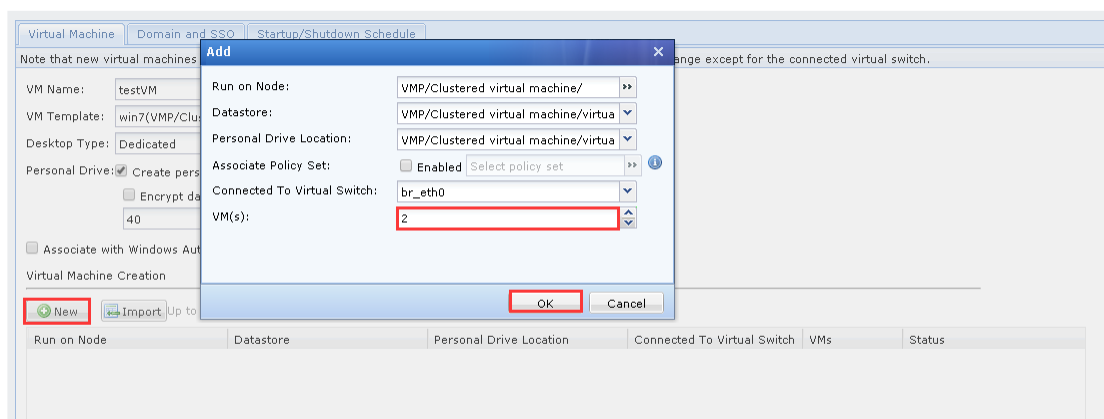
2.3 Creare una risorsa e aggiungere la macchina virtuale al dominio

1. Vai a **VDI Options > Resources > New > Virtual Desktop**, inserisci il nome della risorsa, il nome della VM, il VM Template e il tipo di desktop come da figura seguente:

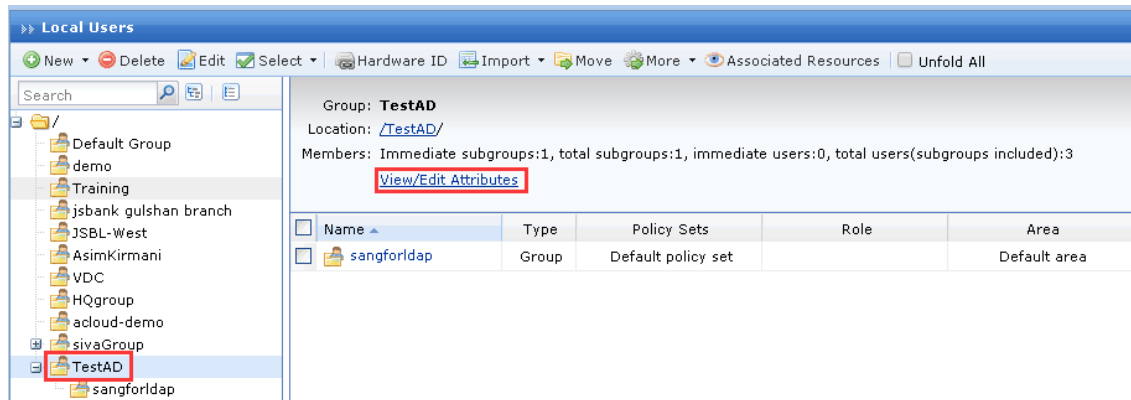


Nota: I Template utilizzati dagli utenti di dominio supportano solo il Template di sistema Windows

2. In **VirtualMachine**, fare clic sul pulsante **Aggiungi** e aggiungere le VM desiderate come da figura seguente:



3. Quando vengono create le VM, vai su **VDI Options > Users**, scegli il gruppo e fai clic su **View/Edit Attributes**. Dopodiché nel campo **Assigned Roles**, clicca su **Create and Associate** per creare un nuovo ruolo.



>> Edit User Group

Basic Attributes

Name: *

Description:

Added To: >>

Area: >> ⓘ

Max Concurrent Users: (0 indicates no limit)

Status: ☒ Enabled ☐ Disabled

☐ Inherit parent group's attributes

☐ Inherit authentication settings

☐ Inherit policy set

☐ Inherit assigned roles

Authentication Settings

Primary Authentication

☐ Local password

☐ Certificate/USB key

☒ External LDAP/RADIUS ▾

Require: ☒ Both ☐ Either

Secondary Authentication

☐ Hardware ID

☐ SMS password based

☐ Dynamic token ▾

☐ Enforce its users/subgroups to inherit the authentication settings

Policy Set

Policy Set: >>

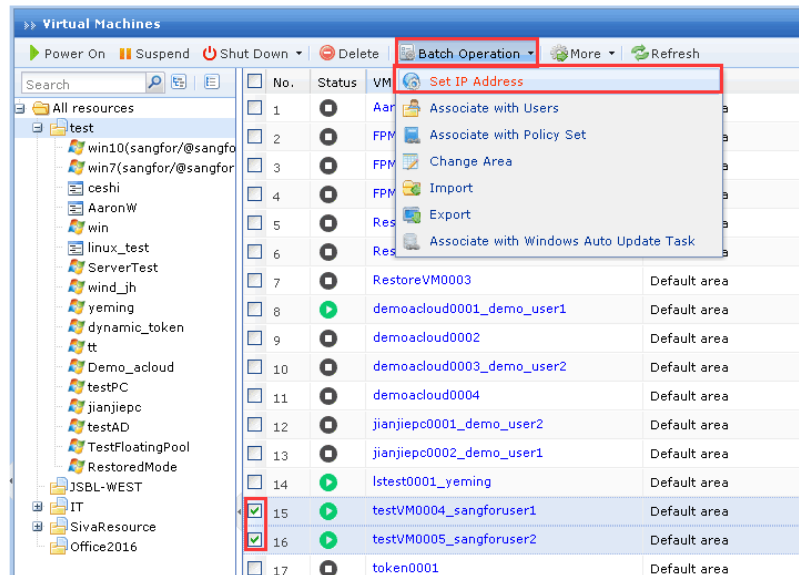
☐ Enforce its users/subgroups to inherit the policy set

Assigned Roles

Roles: >> [Create and Associate](#)

- Inserisci le informazioni, quindi fai clic sul pulsante **Select Resource** per scegliere la risorsa che hai creato nel punto precedente. Premere il pulsante **Save** per salvare e creare il ruolo. Dopo che il ruolo è stato creato e selezionato, fare clic sul pulsante **Save** per salvare gli attributi del gruppo.

6. Dopo l'accensione di queste VM e lo stato diventa di colore **verde**, selezionarle nuovamente e fare clic su **Batch Operation > Set IP Address**.



Nota: Se lo stato diventa verde significa che l'attività dell'agente è normale

7. Assegnare un indirizzo IP per VM: è possibile impostare un IP/DHCP su VDC o configurare manualmente un indirizzo IP statico per VM.

In questo scenario, il metodo di operazione batch viene utilizzato per assegnare un indirizzo IP per le macchine virtuali. Dopo aver specificato l'indirizzo IP, la macchina virtuale deve essere riavviata, quindi è necessario che la casella **Restart VM(s) now** sia selezionata.

Set IP Address

You have selected 2 virtual machine(s). The first two octets of start IP and end IP must be the same.

☐ Specified by user
☐ Auto assigned using DHCP
☒ Specified below

Start IP: 189
 End IP: .190
 Netmask: 255.255.255.0
 Gateway: .1
 Preferred DNS: 33
 Alternate DNS:

☒ Restart VM(s) now (to have IP address change take effect)

OK Cancel



Nota: Per aggiungere la VM al dominio, è necessario che l'indirizzo IP della VM sia in grado di eseguire il ping del nome del dominio (la VM deve essere in grado di risolvere il nome di dominio), anche il server di dominio deve poter eseguire il ping alla VM.

8. Per modificare le risorse, andare su **VDI Options > Resources**, fare clic sulla risorsa. Su **Domain and SSO**, fare clic su **Join VM to AD domain** e inserire i dettagli del server. Infine clicca su **Auto login to PC**, quindi scegli **Domain User**; inserisci il nome del dominio e seleziona **Login as domain user**. Finalmente è possibile fare clic sul pulsante **Test connection** per testare la connettività.

Join VM to AD domain

Server Address: 192.168.1.33
 Server Domain Name: TEST.local
 Admin CN: admin
 Admin Password: *****
 AD Domain OU: OU=sangforidap,DC=TEST,DC=local

Add login to PC

Local user
 Username: Administrator

Domain user (to use domain user account to auto login to computer, join the VM to AD domain first)
 Server Domain Name: TEST.local

☒ Login as domain user (this is only applicable to domain users that are associated with virtual machine)

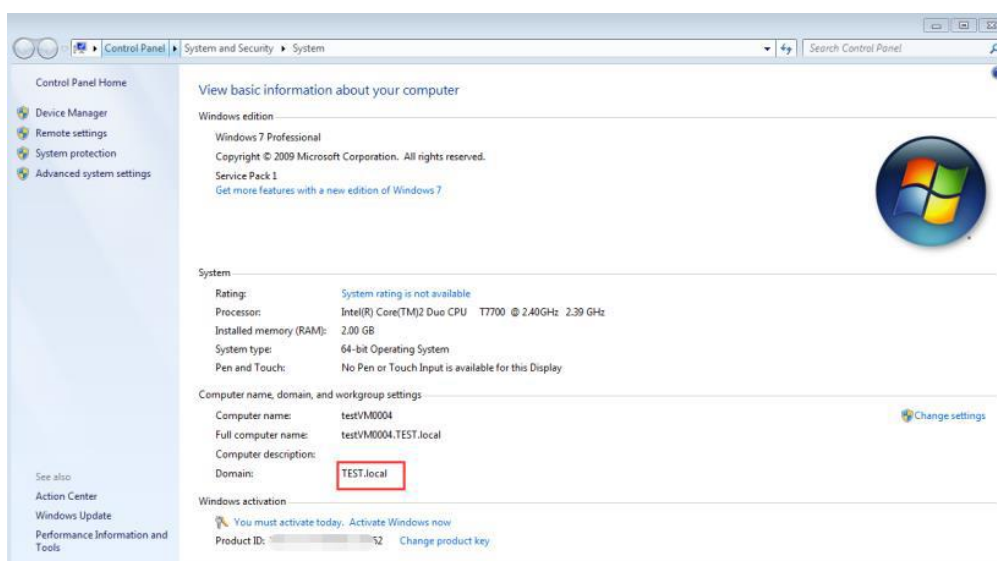
Domain User Permissions
 Join to Administrators Group

Notes:
 1. If VM is in domain, changes to server IP address and domain name take effect after virtual machine is removed from domain and restarted and users relogin.
 2. Changes to OU take effect after virtual machine is removed from domain and restarted, virtual machines are deleted from that OU and users relogin.
 3. For changes to other options, they take effect after users relogin to VDC.

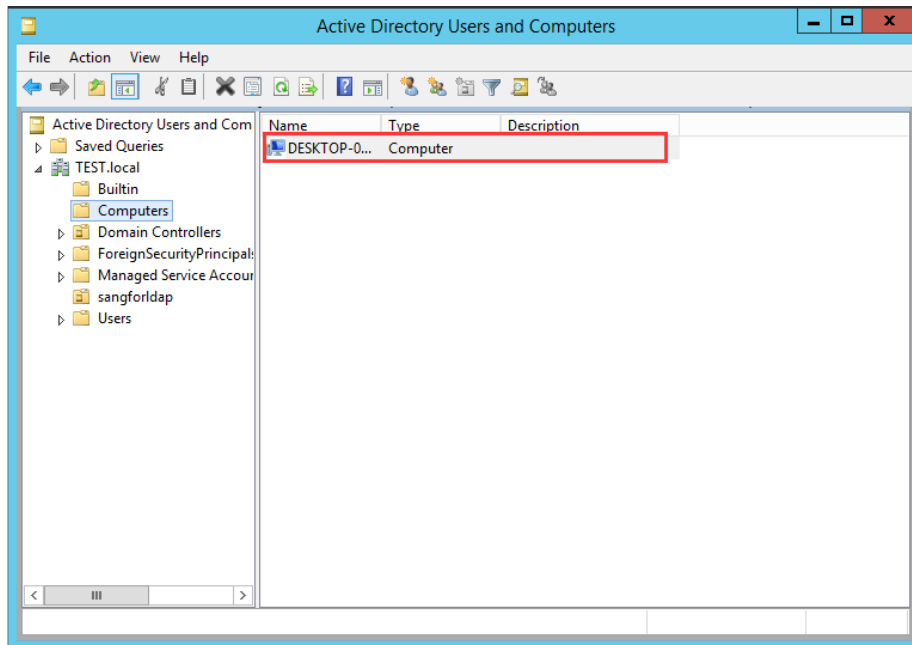


Nota: L'Admin CN è l'account amministratore del server di dominio, non è necessario aggiungere un nome di dominio. Esempio, se l'account dell'amministratore del server è admin e il nome di dominio è TEST.local, allora Admin CN è admin.

9. Aprire il VDI Client, inserire il nome utente e la password del dominio per accedere. Dopo l'accesso, sarà possibile vedere la risorsa e fare clic sulla stessa, quindi sarà possibile accedere alla macchina virtuale.
10. Dopo aver effettuato l'accesso alla VM, è possibile verificare se la VM è associata al dominio oppure no.



11. Andare sul server di dominio, in AD nella cartella **Computers** controlla se la VM è presente nell'elenco dei computer. Se sì, significa che la macchina virtuale è stata aggiunta correttamente al dominio.



Nota: Per la versione VDI precedente alla 5.2, quando si accede per la prima volta alla risorsa, verrà prima eseguita l'associazione al dominio e successivamente sarà eseguito automaticamente un riavvio, quindi solo dopo il riavvio la risorsa si unirà al dominio. Versione successive alla 5.2, il dominio verrà aggiunto al primo accesso alla risorsa, non è necessario riavviare.

2.4 Introduzione e configurazione dell'ottimizzazione del dominio AD

Precauzioni:

1. Sono supportate solo le VM che eseguono il sistema operativo Windows, queste vengono automaticamente aggiunte al dominio.

2. Il Template non è necessario per l'aggiunta a un dominio, la macchina virtuale creata deve essere in grado di eseguire il ping al nome del dominio e anche il server di dominio deve essere in grado di eseguire il ping alla macchina virtuale.

2.4.1 Aggiunta di una VM ad una OU specificata

Configurare la macchina virtuale per l'aggiunta all'OU specificata e impostare i permessi per diverse OU nel Controller di Dominio per facilitare la gestione dei diritti. Per impostazione predefinita, la VM verrà posta nell'OU Computer.

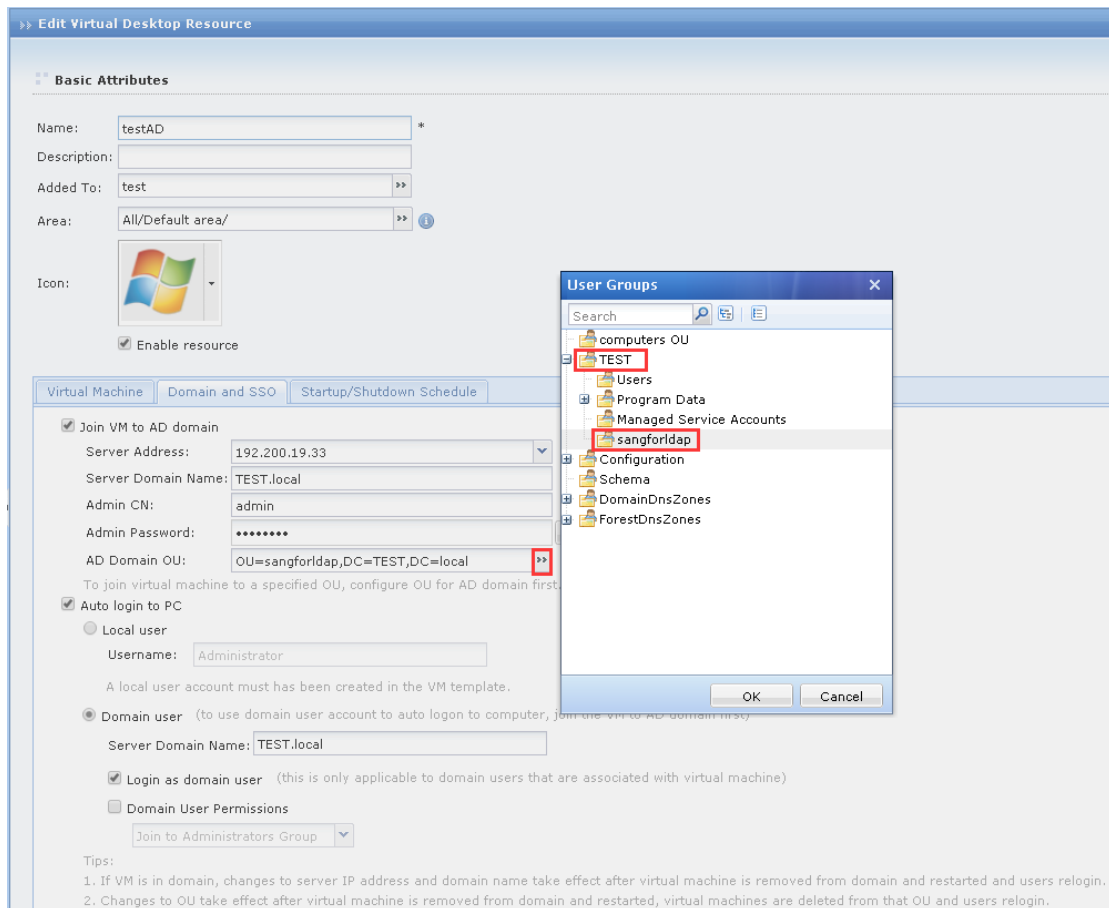
Versione supportata: VDI 5.3.0 e successive.

Requisiti di configurazione

Dopo che la macchina virtuale è stata aggiunta al dominio, cambia l'OU nel dominio. Dopo il cambio dell'OU, è necessario uscire manualmente dal dominio, quindi riavviare la VM ed eliminare la VM originale. Infine, disconnettiti e riconnettiti di nuovo.

Modalità di configurazione:

In VDC, vai a **VDI Options > Resources**, quindi seleziona la risorsa e vai a **Domain and SSO**. Fare clic sul pulsante accanto al campo **AD Domain OU**, verranno mostrate le informazioni sul dominio e selezionare la OU desiderata. Fare clic sul pulsante **Save** per salvare.



2.4.2 Accesso automatico dell'utente di dominio

Versione supportata: Tutte le versioni.

Requisiti di configurazione: Disconnettere l'utente VDI ed effettuare di nuovo l'accesso.

Modalità di configurazione:

In VDC, vai a **VDI Options > Resources**, quindi scegli la risorsa. Dopo aver fatto clic sulla risorsa, vai su **Domain and SSO**, quindi fai clic sulla casella **Join VM to AD domain** per selezionarla ed inserisci le informazioni sul server. È possibile verificare la connettività premendo sul pulsante **Test Connectivity**. Dopodiché fai clic sulla casella **Auto login to PC** per selezionarla, clicca su **Domain User** e nel campo "Server Domain Name" inserisci il nome del dominio. Infine seleziona la casella **Login as domain user**. In ultimo fai clic sul pulsante **Save**.

Edit Virtual Desktop Resource

Description:

Added To: Default group

Area: All/Default area/

Icon:

☒ Enable resource

Virtual Machine | Domain and SSO | Startup/Shutdown Schedule

☒ Join VM to AD domain

Server Address: 192.200.19.45

Server Domain Name: TEST.local

Admin CN: admin

Admin Password: *****

AD Domain OU: OU=sangforidap,DC=TEST,DC=local

Test Connectivity

☒ Auto login to PC

To join virtual machine to a specified OU, configure OU for AD domain first.

☒ Local user

Username: TEST.local

A local user account must have been created in the VM template.

☒ Domain user (to use domain user account to auto login to computer, join the VM to AD domain first)

Server Domain Name: TEST.local

☐ Login as domain user (this is only applicable to domain users that are associated with virtual machine)

☐ Domain User Permissions

Join to Administrators Group

Tips:

1. If VM is in domain, changes to server IP address and domain name take effect after virtual machine is removed from domain and restarted and users relogin.
2. Changes to OU take effect after virtual machine is removed from domain and restarted, virtual machines are deleted from that OU and users relogin.
3. For changes to other options, they take effect after users relogin to VDC.

Save Cancel

2.4.3 Associare l'accesso dell'utente di dominio

Dopo aver configurato l'accesso dell'utente di dominio, solo l'account VDI associato è autorizzato ad accedere alla macchina virtuale. Agli altri utenti di dominio è vietato l'accesso alla macchina virtuale.

Versione supportata: VDI 5.3.0 e versioni successive.

Requisiti di configurazione: Disconnettere l'utente VDI, le modifiche avranno effetto dopo aver effettuato la riconnessione.

Modalità di configurazione:

Su VDI, vai su **VDI Options > Resources**, seleziona la risorsa e vai su **Domain and SSO**, fai clic su **Login as domain user**. Prima di selezionare **Login as domain user**, l'amministratore deve prima aggiungere la VM al dominio e configurare l'accesso automatico al PC.

2.4.4 L'utente di dominio si unisce automaticamente al gruppo Administrators locale o Power Users.

Per impostazione predefinita gli utenti di dominio hanno solo i normali diritti utente, quando è necessario dare agli utenti i permessi per installare software, questo può essere fatto configurando l'utente di dominio ad unirsi al gruppo degli amministratori locali o al gruppo Power Users. Questo permetterà agli utenti di avere diverse autorizzazioni e permessi.

Quando questa opzione è configurata, gli utenti di dominio si uniranno automaticamente al gruppo degli amministratori locali o al gruppo Power Users, assegnando all'utente i privilegi e permessi dei gruppi menzionati.

Dopo aver de-selezionato le opzioni gli utenti di dominio vengono automaticamente rimossi dal gruppo corrispondente, sarà ripristinata l'autorizzazione utente normale e non avrà più l'autorizzazione dei gruppi amministratore locali o Power Users.

Versione supportata: VDI 5.3.0 e versioni successive.

Requisiti di configurazione: Disconnettere l'utente VDI, le modifiche avranno effetto dopo aver effettuato la riconnessione.

Modalità di configurazione:

In VDC, vai a **VDI Options > Resources**, quindi scegli le risorse e vai a **Domain and SSO**. Nel campo **Auto login to PC**, clicca sulla casella **Domain User Permissions** e nel menu a tendina

puoi scegliere che permessi impostare: **Join to Administrators Group** o **Join to Power Group**. L'amministratore deve prima aggiungere la macchina virtuale al dominio e configurare l'accesso automatico al PC.

Edit Virtual Desktop Resource

Description:

Added To:

Area:

Icon:

☒ Enable resource

Domain and SSO

☒ Join VM to AD domain

Server Address:

Server Domain Name:

Admin CN:

Admin Password:

AD Domain OU:

To join virtual machine to a specified OU, configure OU for AD domain first.

☒ Auto login to PC

☐ Local user

Username:

A local user account must has been created in the VM template.

☒ Domain user (to use domain user account to auto logon to computer, join the VM to AD domain first)

Server Domain Name:

☐ Login as domain user (this is only applicable to domain users that are associated with virtual machine)

☒ Domain User Permissions

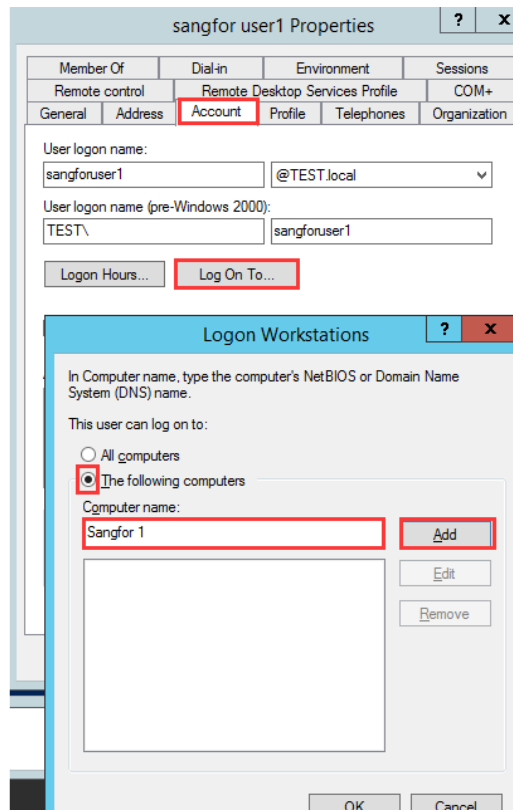
Tips:

1. If VM address and domain name take effect after virtual machine is removed from domain and restarted and users relogin.
2. Changes to OU take effect after virtual machine is removed from domain and restarted, virtual machines are deleted from that OU and users relogin.
3. For changes to other options, they take effect after users relogin to VDC.

2.4.5 Altre caratteristiche.

Versione supportata: VDI 5.2 e versioni successive

1. Supporta l'accesso al nome del computer con l'associazione al nome dell'utente di dominio, ovvero l'accesso dell'utente di dominio al nome computer specificato.



2. Gli utenti di dominio non fanno distinzione tra maiuscole e minuscole.

Quando un utente di dominio accede ad una risorsa, viene automaticamente convertito in caratteri minuscoli nella VM associata. Questa modifica ha effetto solo per l'utente di dominio e non influisce sull'utente locale. Dopo l'importazione dell'utente di dominio, il nome utente viene modificato in minuscolo. L'utente di dominio è ancora connesso, ovvero la password viene salvata nel server di dominio.



Nota: Il VDC è stato configurato con l'autenticazione di dominio LDAP, se il dispositivo VDC ha un utente di dominio in maiuscolo nella VM associata, l'autenticazione fallirà.

(Nelle versioni successive alla 5.2 avrà effetto)

Capitolo 3: Descrizione della registrazione (LOG) dei processi effettuati

Processo di aggiunta al dominio:

1. Avviare la risorsa, avvio dell'aggiornamento di Windows, riavviare una volta completato l'aggiornamento.
2. Appena avvio completato, fare aggiunta al dominio, dopo l'aggiunta al dominio, riavviare.

A. Registro (Log) della Configurazione dell'aggiunta al dominio:

C:\Windows\Temp\vdagent.log

[INFO] [VDAgent::HandleLogon] rcv windows logon info, addlocal flag:33554432 domain:adserver53.com,binddomain flag:16777216 domain:adserver53.com user:ad_1

B. Registro (Log) dei risultati dell'aggiunta al dominio:

C:\Programmi\Sangfor\SSL\VDI\Logs\VDNetdom.log

[VDNetdom] 0.JoinDomain of adserver53.com is succ. [INFO]
[VDNetdom] Join in domain(adserver53.com) successful, we need to reboot system.

C. Registro (Log) dell'associazione dell'utente:

C:\Windows\Temp\vdagent.log

[INFO] [SetBindDomain]Bind domain, loginmod:2 flag:1 domain:adserver53.com user:ad_1



Nota: 1= Binding, 0= Non binding

D. Registro (Log) dell'aggiunta al gruppo di gestione:

C:\Windows\Temp\vdagent.log

[INFO] [AddLocalGroup] Add local group, loginmod:2 flag:2

domain:adserver53.com user:ad_1

[INFO] [AddLocalGroup] LastUser: CurrentUser: AddFlag:2



Nota: 0 = Not aggiunto, 2 = gruppo di gestione locale, 4 = gruppo Power Users

[INFO] [DelUserFromGrp] Delete User from Grp ret 2226



Nota: Prima cancella la vecchia relazione al gruppo di utenti.

[INFO] [AddUserToGrp] Add User to Grp fail, ret 2226



Nota: Aggiunta di una nuova relazione al gruppo di utenti.

3. Avvio completato, accesso automatico.

Registro di accesso automatico:

C:\Windows\System32\LogonUI.log (xp:
c:\windows\system32\winlogon.log)

3.1 Prima verificare se esiste una relazione di trust (trust relationship):

[PID:00760 TID:01116] [DBG] [VDSSO]

IsMyComputerOnDomainTrust pszDomain:ADSERVE

3.2 Relazione di trust esistente:

**[PID:00760 TID:01116] [INFO] [VDSSO] [TC_QUERY]netlog 2_flags:48,
trusted_dc_name:\\vdit.adserver53.com, status:0**

[PID:00760 TID:01116] [INFO] [VDSSO] [TC_VERIFY]netlog

2_flags:176, trusted_dc_name:\\vdit.adserver53.com, status:0

3.3 Abilitare l'accesso all'avvio:

[PID:00760 TID:01116] [INFO] [VDSSO] Computer has join domain, will Autologin system

Capitolo 4 Problemi comuni

4.1 Aggiunta VM a domino / aggiunta a OU non riuscito

1. Controllare la configurazione dell'aggiunta ad AD domino della VM nel VDC

Controllare la configurazione VDC in **Domain and SSO**, verificare l'indirizzo IP del server, il Domain Name Admin CN, la password e così via.

2. Verificare se la VM può raggiungere il dominio oppure no, il DNS deve essere in grado di risolvere il nome di dominio.

È necessario assicurarsi che la VM sia in grado di eseguire il ping del nome del dominio, anche il server di dominio deve eseguire il ping all'IP della VM. Il DNS della VM deve essere in grado di risolvere il nome del dominio.

3. Provare ad aggiungere manualmente la macchina virtuale al dominio.
4. Analisi dei registri (log):

1. Se la configurazione del VDC è corretta, verificare se la configurazione viene distribuita correttamente.

Se l'utente locale ha effettuato l'accesso alla VM, controllare il registro di recapito: C:\Windows\Temp\vdagent.log. Se la configurazione non corrisponde al seguente formato, nessun dominio o utente, la configurazione è sbagliata.

**[VDAgent::HandleLogon] rcv windows logon info, addlocal
flag:33554432 domain:adserver53.com, binddomain flag:16777216
domain:adserver53.com user:ad_1**

2. Se la configurazione viene distribuita correttamente, verificare se il processo di aggiunta al dominio è anormale. Accedere alla VM come utente locale, visualizzare il log di configurazione ed aprirlo direttamente dalla VM.
3. %VDI%\Logs\VDNetdom.log, %VDI%\Logs\VDAgent.log

1. La VM è aggiunta correttamente al dominio e deve essere riavviata per avere effetto.

[VDNetdom] Join in domain(micota) successful, we need to reboot system.

2. La VM è stata aggiunta al dominio e non è necessario aggiungerla nuovamente al dominio.

[Agent] The computer is already in domain.

3. La VM non è riuscita a risolvere il nome del dominio, potrebbe essere causato dall'assegnazione dell'IP dal server DHCP non riuscito, l'IP specificato non ha effetto o l'IP assegnato non può raggiungere il dominio.

```
[INFO] [VDNetdom] CurrentLocalIP:127.0.0.1
[ERROR] [VDNetdom] gethostbyname is fail.Err:11004
<DBG> [VDNetdom] 0.TryConnect of son.adserver53.com return:0
```

4. Aggiunta alla OU Computer di dominio non riuscita.

Nella VM aprire il file di registro (log) %VDI%\Logs\VDNetdom.log e cercare su internet soluzioni correlate ai vari messaggi di errore.

5. Verificare se la VM è stata aggiunta al dominio o se è stata aggiunta al dominio in precedenza, è presente un nome computer residuo nell'unità organizzativa del dominio.
6. Se nessun problema sopra descritto risolve i problemi di aggiunta al dominio, si prega di contattare R&D.

4.2 Desktop virtuale aggiunto al dominio ma

accesso automatico al dominio non riuscito

1. Verificare che il desktop virtuale sia stato aggiunto al dominio di Active Directory.
2. Prova ad inserire manualmente il nome utente e la password del dominio AD per accedere.
3. Prova ad utilizzare il servizio RDP per accedere.
4. Utilizza il messaggio di errore al prompt per cercare sui motori di ricerca una soluzione.

4.3 Errore nell'aggiunta al gruppo di gestione locale

1. Controllare la configurazione.
2. Controllare il registro.
3. Visualizza il processo di aggiunta al gruppo di gestione. Se il registro non soddisfa le condizioni di cui sopra, la causa dell'errore è nota in base al contenuto del campo del registro di stampa.

4.4 La funzione di associazione è in errore

1. Controllare la configurazione.
2. Controllare il registro (log)in: C:\Windows\Temp\vdagent.log
**[INFO] [SetBindDomain] Bind domain, loginmod:2 flag:1
domain:adserver53.com user:ad_1**
3. Controllare il registro di sistema e verificare se ci sono informazioni sull'associazione

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SfSysPrep\C
PUI D**

Binddomain = adserver53.com, binding domain.

Isbindvmuser = 1, se binding oppure no. 1 = binding, 0 = not binding

Username = ad_1, binding user.

4.5 Errore di accesso automatico



Nota: la relazione di trust tra i server di dominio AD e la VM non è riuscita, verificare se il server di dominio AD è online o provare a riavviare il computer.

1. Controlla la configurazione, assicurati che il nome utente e la password siano corretti.
2. Controllare il registro (log) in: C:\Windows\System32\LogonUI.log

```
[DBG] [VDSSO] IsMyComputerOnDomainTrust pszDomain:ADSERVER53  
[INFO] [VDSSO] [TC_QUERY]netlog 2_flags:0, trusted_dc_name:, status:1311  
[INFO] [VDSSO] Computer do not join domain, but will not login system.  
[INFO] [VDSSO] CurrentLocalIP:199.201.134.241
```

Se la relazione di trust non riesce, si verificano due situazioni:

1. Come dice il registro, la macchina virtuale non fa parte del dominio.
2. La macchina virtuale è stata aggiunta al dominio, ma il test di comunicazione con il server di dominio non riesce. Dopo l'avvio, in background, tenterà di connettersi al server di dominio 10 volte (1 volta al secondo). In caso di errore, verrà registrato il seguente messaggio.

```
[DBG] [VDSSO] CSSOProvider::GetCredentialCount VdeskMode:1,  
iTryCount:10, wszUserName:adserver53.com\ad_2, SSOLogMode:2
```

```
[DBG] [VDSSO] IsMyComputerOnDomainTrust pszDomain:ADSERVER53
```

```
[INFO] [VDSSO] [TC_QUERY]netlog 2_flags:0, trusted_dc_name:,  
status:1787
```



Nota: saranno registrati 10 messaggi come sopra.

[INFO] [VDSSO] Computer do not join domain, but will not login system.

[INFO] [VDSSO] CurrentLocalIP:199.201.134.241

Questo è un problema di rete, è possibile accedere correttamente dopo aver utilizzato l'accesso manuale con l'utente del dominio.

Se l'accesso non riesce ancora, si prega di contattare il supporto tecnico per assistenza.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc