

FUTURE DECODED

6-7 OTT '16 / MILANO

IN PARTNERSHIP WITH:  CommunityDays.it

www.futuredecoded.it

 #FutureDecoded

Remote Desktop Services stato dell'arte e novità in Windows Server 2016 e Azure

Ermanno Goletto

MVP Cloud and Datacenter Management

MVP Enterprise Mobility

<http://www.devadmin.it>

Roberto Massa

MVP Cloud and Datacenter Management

<http://massarobi.wordpress.com>

ICT  POWER.IT


www.futuredecoded.it

 [#FutureDecoded](https://twitter.com/FutureDecoded)

Agenda

- Architettura RDS
- Gestione RDS e VDI
- Novità in Windows Server 2016
- RDS Security e Troubleshooting

FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

A nighttime photograph of a city street with tall buildings and light trails from traffic. The image is split vertically: the left side shows a street with a blue tint, and the right side shows a highway with red and white light trails from cars. The text is overlaid on the left side.

Architettura RDS

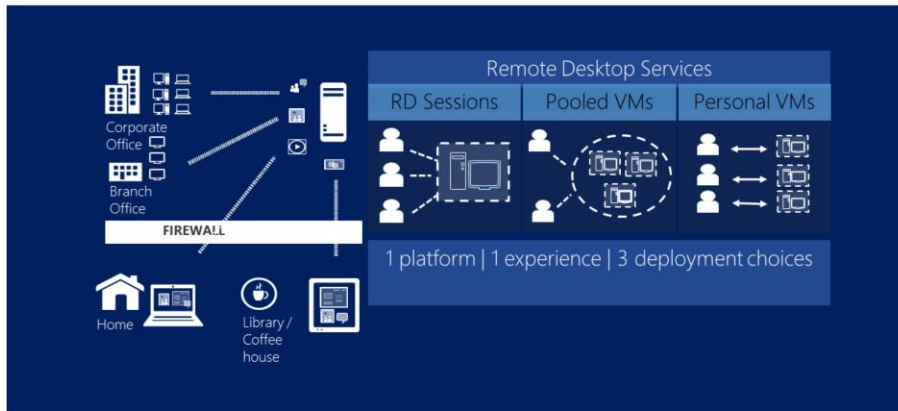
Remote Desktop Services
stato dell'arte e novità in
Windows Server 2016 e Azure

www.futuredecoded.it



#FutureDecoded

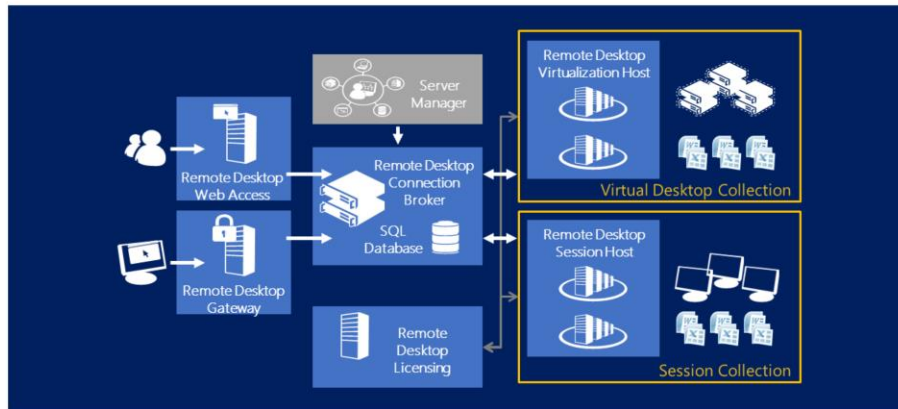
Architettura infrastruttura RDS



FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

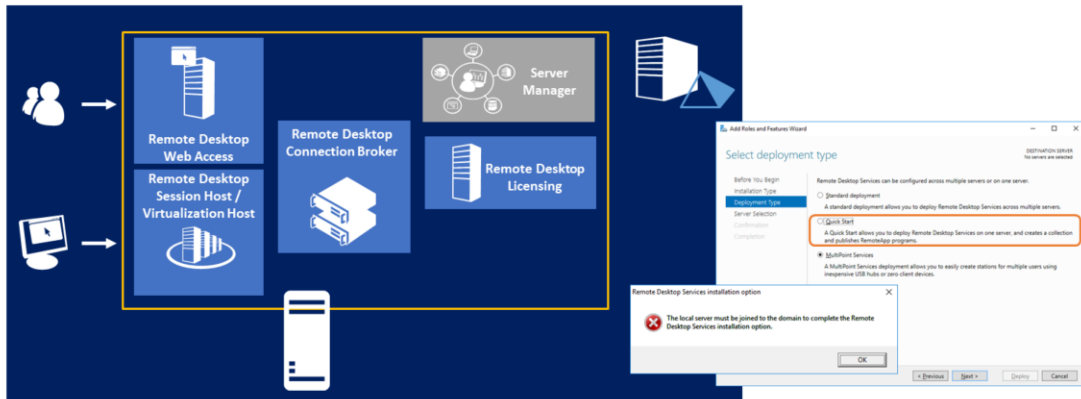
Componenti di un'infrastruttura RDS




FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Architettura per piccole infrastrutture



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Componenti di un'infrastruttura

Windows Server 2012

- Non è supportato installare i ruoli RDS e i ruoli AD DS sullo stesso computer (KB2799605), in quanto non è possibile installare il ruolo RD CB insieme al ruolo AD DS
- Se vi è un solo server nella rete è possibile installare il solo ruolo RD SH insieme al ruolo AD DS (KB 2833839)
- Senza il ruolo RD CB non sarà possibile avere le funzionalità complete degli RDS (le Remote App non saranno disponibili)



Windows Server 2012 R2

- E' supportato installare il ruolo RD CB insieme al ruolo AD DS, quindi è possibile avere un unico server DC+RDS
- In scenari Workgroup non è possibile utilizzare Server Manager per la gestione degli RDS, occorre utilizzare PowerShell ed è necessario il FQDN



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

<http://blogs.msdn.com/b/rds/archive/2013/07/09/what-s-new-in-remote-desktop-services-for-windows-server-2012-r2.aspx>

RDS e Windows Server Essentials

Conviene
acquistare
una STD

Novità in Windows Server 2012

- Essentials è diventato un ruolo in WS2012 R2 STD/DC
- La feature Remote Web Access non richiede RDS CAL
- Essentials supporta solo il ruolo RD Gateway, richiesto da Remote Web Access e non richiede RDS CAL
- Le RDS CAL sono richieste se si usano funzionalità RDS esposte da WS2012 R2 STD o DC anche tramite il ruolo Essentials

Implementazione tramite VM Essentials e VM RDS



<http://blogs.technet.com/b/sbs/archive/2013/09/03/understanding-licensing-for-windows-server-2012-r2-essentials-and-the-windows-server-essentials-experience-role.aspx>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

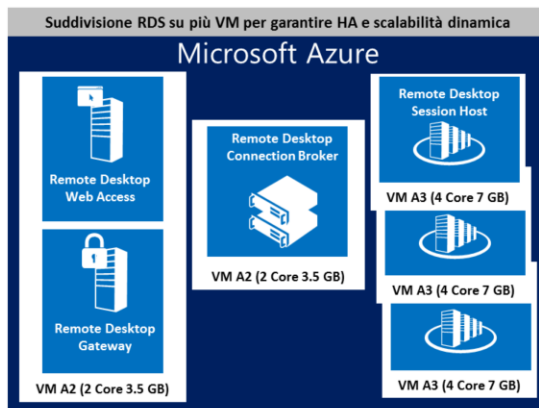
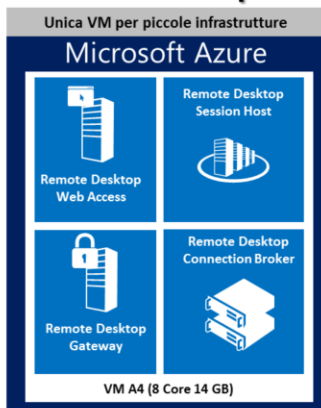
<http://www.microsoft.com/licensing/about-licensing/briefs/terminal-services.aspx>
<http://blogs.technet.com/b/sbs/archive/2013/09/03/understanding-licensing-for-windows-server-2012-r2-essentials-and-the-windows-server-essentials-experience-role.aspx>

<http://blogs.sysadmin.it/ermannog/archive/2013/07/09/windows-server-2012-active-directory-e-ruoli-rds.aspx>

<http://blogs.technet.com/b/sbs/archive/2012/12/12/using-windows-server-2012-essentials-with-more-than-25-users.aspx>

<http://technet.microsoft.com/en-us/library/jj628148.aspx>

Scenari per RDS su Microsoft Azure



Dal 1 gennaio 2014 le RDS CAL con SA attiva possono avvalersi degli RDS CAL Extended Rights che consentono l'uso delle RDS CAL anche su WS in esecuzione in Microsoft Azure

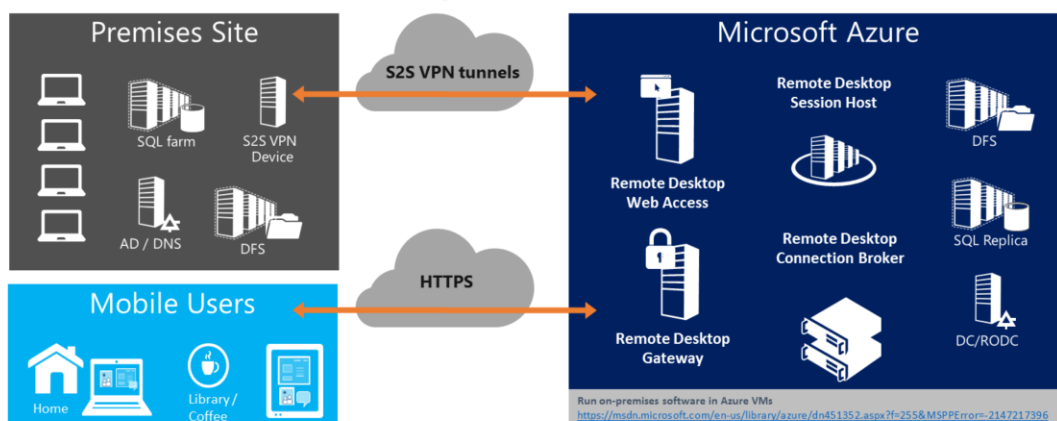
Le VM create tramite un template della Azure virtual machine gallery comprendono le CAL nella tariffa

Azure Desktop Hosting - Reference Architecture and Deployment Guides: <https://msdn.microsoft.com/en-us/library/azure/dn451351.aspx>


**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

Soluzione RDS Hybrid Cloud su Azure



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Reference Architecture per RDS

<https://msdn.microsoft.com/en-us/library/azure/dn451351.aspx>

Active Directory su Azure VMs

<https://msdn.microsoft.com/en-us/library/azure/dn151466.aspx>

SQL Server su Azure VMs

<https://msdn.microsoft.com/en-us/library/azure/jj823132.aspx>

Esecuzione di on-premises software su Azure VMs

<https://msdn.microsoft.com/en-us/library/azure/dn451352.aspx>

Scenari Azure di test

<https://www.microsoft.com/italy/azureboxes/>

Azure RemoteApp

Sostituite con le Citrix XenApp «express»

- Saranno supportate fino al 31 Agosto 2017
- La vendita è cessata il 1 Ottobre 2016
- Verrà fornito supporto ai clienti per la transizione
- Una technical preview delle XenApp “express” è prevista nell’ultimo trimestre del 2016



"Customers have provided us consistent feedback that they want a comprehensive, end-to-end, cloud-based solution for delivering Windows apps. The best way for us to deliver this is with Citrix through XenApp "express", currently under development. XenApp "express" combines the simplicity of application remoting and the scalability of Azure with the security, management, and performance benefits of XenApp, to deliver Windows applications to any employee on any device. We will have much more to share on this offering through the coming months."

Remote Desktop Team – 12 Agosto 2016

"In conjunction with this effort, Microsoft recently announced its intent to take the next step in its broad partnership with Citrix, by assisting us in developing the next generation of the Azure RemoteApp service. This future Citrix XenApp "express" offering will combine the simplicity and speed of Microsoft Azure RemoteApp with many of the enterprise capabilities of Citrix XenApp to revolutionize app delivery from the cloud."

Bill Burley Citrix corporate vice president – 12 Agosto 2016

**FUTURE
DECODED | MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<https://blogs.technet.microsoft.com/enterprisemobility/2016/08/12/application-remoting-and-the-cloud/>

<https://www.citrix.com/blogs/2016/08/12/citrix-to-introduce-a-cloud-service-that-delivers-secure-apps-from-azure-to-any-device/>

<https://rcpmag.com/articles/2016/08/12/microsoft-replacing-azure-remoteapp.aspx>

<http://www.zdnet.com/article/microsoft-to-drop-azure-remoteapp-in-favor-of-citrix-remoting-technologies/>

<https://www.citrix.com/blogs/2016/08/15/an-open-letter-to-microsoft-azure-remoteapp-customers/>

<https://www.citrix.com/blogs/2016/08/22/citrix-and-microsoft-delivering-on-our-promises/>



A nighttime photograph of a city street with tall buildings and light trails from traffic. The image is split vertically: the left side shows a dark street with light trails, and the right side shows a brightly lit highway with a bridge and light trails.

Gestione RDS e VDI

Remote Desktop Services
stato dell'arte e novità in
Windows Server 2016 e Azure

www.futuredecoded.it



#FutureDecoded

VDI vs Session Virtualization

	Virtual Desktop Infrastructure	Session Virtualization
Isolamento sistema operativo	✓	✗
Compatibilità applicativa nativa elevata	✓	✗
Diritti amministrativi sul desktop remoto	✓	✗
Delivery singola LOB application	✗	✓
Miglior scalabilità (densità utenti per server)	✗	✓
Minor hardware e gestione server	✗	✓
Minor CAPEX (spesa per acquisto asset) per user	✗	✓
Minor OPEX (spesa per gestione asset) per user	✗	✓
Personalizzazione granulare del desktop	✓	✗
Rich desktop experience tramite RemoteFX	✓	✓

FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Deploy RDS e VDI

Centralizzazione e deploy dedicato

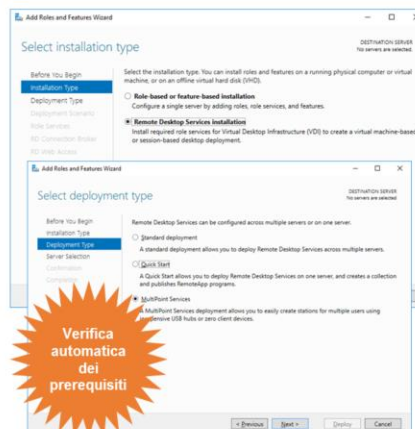
- Server Manager come unica console di deploy e amministrazione sia locale che remota
- Opzione dedicata a RDS nel wizard Add Roles
- Modalità Standard (deploy scalabile)
- Modalità Quick Start (deploy a singolo server)
- Modalità MultiPoint (deploy shared computer)

Quick Start Virtual machine-based

- Ruolo RD Connection Broker
- Ruolo RD Web Access
- Ruolo RD Virtualization Host

Quick Start Session-based

- Ruolo RD Connection Broker
- Ruolo RD Web Access
- Ruolo RD Session Host



FUTURE
DECODED | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Modulo RDS PowerShell

Deploy

Session Collections

Virtual Desktop
Collections

Sessions

RemoteApp e
Desktop

```
# Import del modulo RDS
Import-Module RemoteDesktop
Get-Command -Module RemoteDesktop

# Personalizzazione Titolo pagina web su RD Web Access
Set-RDWorkspace -Name "XYZ Applications" -ConnectionBroker broker01.company.local

# Creazione RemoteApp
New-rdremoteapp -Alias Wordpad -DisplayName WordPad -FilePath "C:\Program Files\Windows NT\Accessories\wordpad.exe"
-ShowInWebAccess 1 -collectionname MySessionCollection -ConnectionBroker LS01.CRFB.Local

# Creazione Folder RemoteApp
Set-RDRemoteApp -CollectionName MySessionCollection -Alias Calculator -FolderName "My Favorite tools" -ConnectionBroker
SH01.CRFB.Local

# Creazione File Type Association
Set-RDFileTypeAssociation -CollectionName MySessionCollection -AppAlias AcrobatReader -FileExtension .pdf -IsPublished $true
-ConnectionBroker SH01.CRFB.Local
```



FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<https://technet.microsoft.com/en-us/library/jj215451.aspx>

Su TP5 Get-Command -Module RemoteDesktop | Measure-Object restituisce 79

Deploy VDI - VM Streaming

Server Manager

- Gestione Master images VMs personal e pooled
- Gestione Streamlined delle VM
- Gestione del patching delle VM
- Pubblicazione RemoteApp da Collection di VMs

- *Per default il provisioning delle VM è seriale*
- *N° provisioning simultanei definito dalla registry key*
HKLM\System\CurrentControlSet\Services\VmHostAgent\Parameters\Concurrency
- *Il valore massimo raccomandato è 5*

Build VM Master Windows 8/8.1/10



- Installare l'OS
- Join della VM al dominio
- Installazione applicazioni
- Avvio PowerShell come amministratore locale
- Esecuzione Sysprep:
`%windir%\system32\sysprep\sysprep.exe`
`/generalize /oobe /shutdown /mode:vm`

Build VM Master Windows 7



- Installare l'OS
- Aggiornamento Integration Services
- Join della VM al dominio
- Installazione applicazioni
- Avvio PowerShell come amministratore locale
- Esecuzione Sysprep:
`%windir%\system32\sysprep\sysprep.exe` `/generalize`
`/oobe /shutdown`

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

<http://blogs.technet.com/b/andrew/archive/2013/10/28/lab-ops-4-windows-8-1-windows-2012r2-vdi.aspx>

<http://blogs.msdn.com/b/rds/archive/2012/10/29/single-image-management-for-virtual-desktop-collections-in-windows-server-2012.aspx>

/mode:vm

New for Windows® 8. Generalizes a Virtual Hard Disk (VHD) so that you can deploy the VHD as a VHD on the same Virtual Machine (VM) or hypervisor. After the VM restarts, the VM can boot to OOBE.

The only additional switches that apply to VM mode are **/reboot**, **/shutdown**, and **/quit**

You can only run VM mode from inside a VM. You cannot deploy the VHD to any computer

<http://blogs.msdn.com/b/rds/archive/2012/07/18/setting-up-a-new-remote-desktop-services-deployment-using-windows-powershell.aspx>

Deploy VDI - Intelligent Patching

Pooled VM

- Aggiornamento del VHD template e redistribuzione tramite RD Connection Broker
- Modalità di patching
 - Attesa log off
 - Definizione deadline oltre la quale viene forzato il log off
 - Log off forzato immediatamente



Personal VM

- Gestito tramite WSUS mentre la VM è attiva
- L'RD CB può operare con System Center Configuration Manager per bilanciare il carico sull'host
- L'RD CB può eseguire il wake up delle VM
 - Deploy Agent SCCM nelle VM
 - SCCM esegue il wake up della VM, installa le hotfixes e rimette in save state la VM



FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

User Profile Disks (UPD)

Cache per User state e application data

- Introdotti con WS2012 per mantenere User state e application data per sessioni RD e nei Virtual Desktop Pool
- Cache per Roaming User Profiles (RUP), Folder Redirection (FR) e User Environment Virtualization (UE-V)
- Mantenimento dati applicazione non memorizzati nel profilo utente
- VHD Montati automaticamente al logon in una sessione RD o VDI Pooled
- Le directory del profilo e dei dati vengono mappate sul volume dello User Profile Disk
- Avvio più rapido (sincronizzazione non necessaria)
- Lo scope degli User Profile Disk è la collection
- Consentono il roaming tra le VM e/o i server RD SH nella Collection

UPD

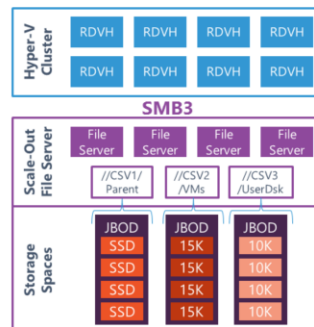
Per ogni VM Pool
e RDSH Collection

UE-V

Roaming dei settings
tra le collections

FR

Roaming dati utente
tra le collections e backup



Completano le funzionalità di centralizzazione di User State e Application Data insieme a:

- Roaming User Profiles (RUP)
- Folder Redirection (FR)
- User Experience Virtualization (UE-V)

FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

Pubblicazione RemoteApp

Metodi di pubblicazione

- Portale web dell'RD Web Access
- RemoteApp and Desktop Connections specificando URL o Email utente
- GPO utente Specify default connection URL in Administrative Templates/Windows Components/Remote Desktop Services/RemoteApp and Desktop Connections
- Il deploy tramite MSI/.Rdp non più supportato

Disponibile in
WS2012/W8 e succ.

General

RemoteApp program name:
Calculator

Alias:
calc

RemoteApp program location:
C:\Windows\system32\calc.exe

Current icon:

Show the RemoteApp program in RD Web Access
Yes ☒ No ☐

RemoteApp program folder:

Type the name of the folder in which you want this RemoteApp program to appear on the RD Web Access server. If you do not want the RemoteApp program to appear in any folder, leave this field blank.



FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

<https://RDWA1.corp.contoso.com/RDWeb/Feed>

<http://technet.microsoft.com/en-us/library/hh831442.aspx>

<http://blogs.msdn.com/b/rds/archive/2013/05/21/windows-server-2012-remoteapp-and-desktop-connections-default-connections-and-file-type-associations.aspx>

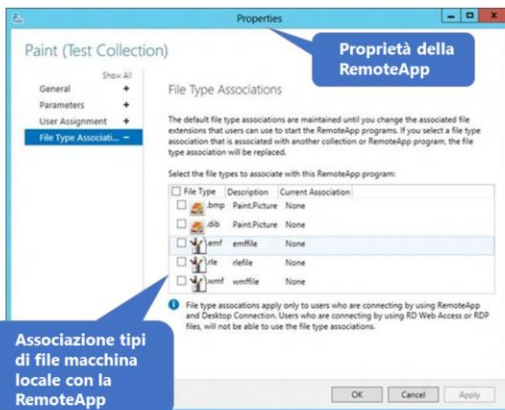
File Type associations

Metodi di deploy

- Server Manager
- PowerShell utilizzando i cmdlets:
 - Set-RDFileTypeAssociation
 - Get-RDFileTypeAssociation
- GPO utente Specify default connection URL

Disponibile in
WS2012/W8 e succ.

Le File Associations vengono applicate solo a RemoteApp pubblicate tramite Remote App and Connections e non tramite RD WebAccess page



<http://blogs.msdn.com/b/rds/archive/2013/05/21/windows-server-2012-remoteapp-and-desktop-connections-default-connections-and-file-type-associations.aspx>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Reset password scadute da RD WA

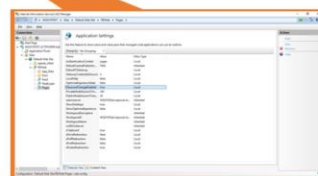
Passi di configurazione

- L'opzione di modifica della password è gestita dalla pagina password.aspx in C:\Windows\Web\RDWeb\Pages\en-US
- Occorre impostare tramite l'IIS Manager la proprietà PasswordChangeEnabled a true nell'Application Settings del Default Web Site

Domain/user name:

Password:

Your password is expired. Click [here](#) to change it.



<https://social.technet.microsoft.com/wiki/contents/articles/10755-windows-server-2012-rds-enabling-the-rd-webaccess-expired-password-reset-option.aspx>

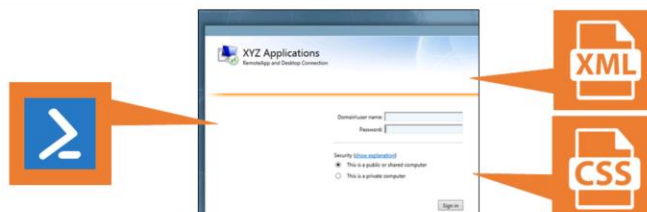
**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Personalizzazione RD Web Access

Opzioni di personalizzazione

- RD Web Access costruisce la pagina web utilizzando il feed XML utilizzato da RemoteApp and Desktop Connections, è possibile eseguire il Re-branding del default web site intervenendo sullo style sheet e sul file xml C:\Windows\Web\RDWeb\Pages\en-US\RDWAStrings.xml
- Per la modifica del Title occorre usare il cmdlet PowerShell Set-RDWorkspace
- E' possibile creare semplicemente estensioni di terze parti



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Gestione stampanti

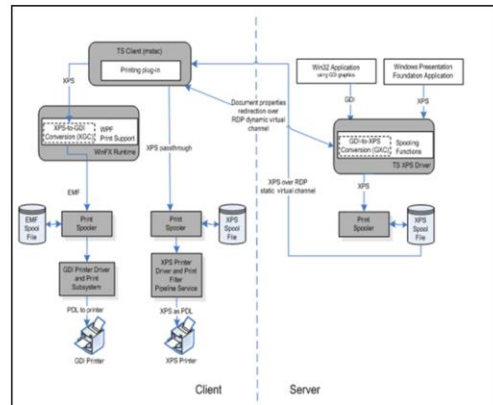
RD Easy Print

- Disponibile in WS2008 TS/WS2008R2 RD SH e succ.
- Richiede RDC 6.1 con .NET 3.0 SP1 o RDC 7 e succ.
- L'RD Session tenta di utilizzare prima il driver Easy Print di Desktop remoto
- Se il client non supporta RD Easy Print si utilizza Printer Redirection cercando un driver della stampante nel server (KB239088)

Disponibile anche nelle edizioni Enterprise di Windows 7 e succ.

Fallback printer driver

- Non più supportato in WS2008 e succ.
- La GPO è applicabile solo a WS2003 SP1/SP2



FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

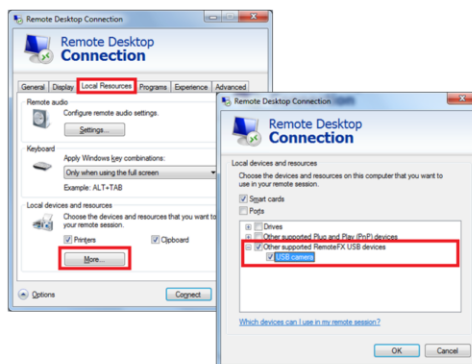
In partnership with:
CommunityDays.it

<https://blogs.technet.microsoft.com/askperf/2008/02/17/ws2008-terminal-services-printing/>

RemoteFx USB Redirection


Funzionalità, requisiti e limitazioni

- Redirige svariati dispositivi USB connessi ad un client
- Driver installati sull'RD SH/VM e non richiesti sul client
- In WS2008R2/W7 il device utilizzabile solo in una singola sessione
- In WS2012/W8 supporto a redirezioni multiple con session isolation
- Richiede RDC 7.1 o succ.
- Non tutti i device USB possono essere redirezionati (KB2653326, KB3125295)



<https://blogs.technet.microsoft.com/enterprisemobility/2012/09/11/remotefx-usb-redirection-in-windows-server-2012-and-windows-8/>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<https://support.microsoft.com/en-us/kb/3125295>

<https://blogs.technet.microsoft.com/enterprisemobility/2012/09/11/remotefx-usb-redirection-in-windows-server-2012-and-windows-8/>

<http://h10032.www1.hp.com/ctg/Manual/c04957360>



A nighttime photograph of a city street with light trails from cars. In the background, several tall skyscrapers are illuminated with blue and white lights. A pedestrian bridge with a pinkish-red railing is visible in the middle ground. The overall scene is dark, with the city lights providing the primary illumination.

Novità in Windows Server 2016

Remote Desktop Services
stato dell'arte e novità in
Windows Server 2016 e Azure

www.futuredecoded.it

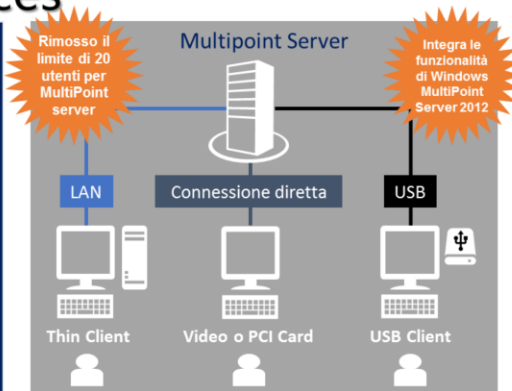


#FutureDecoded

Ruolo MultiPoint Services

Metodi di deploy

- Gli utenti che si connettono al Multipoint Server hanno a disposizione il loro desktop e non un desktop standard condiviso
- Installando il ruolo Multipoint Services viene anche installato il ruolo RDSH
- Il Ruolo Multipoint e il ruolo RDSH operano congiuntamente per ridurre il TCO e fornire la possibilità di usare orchestration tools per la gestione di sessioni RDSH e dei device
- MultiPoint non utilizza/richiede RD Connection Broker e RD Gateway
- Stazioni di lavoro a basso costo vengono connesse all'host shared via USB, video card o LAN



MultiPoint Zero Clients con costi da 25\$ a 50\$ (alcuni non usano RDP)
<http://blogs.technet.com/b/multipointserver/archive/2013/03/07/roundup-of-online-resources-for-windows-multipoint-server-2012.aspx>

<http://blogs.msdn.com/b/rds/archive/2014/10/27/announcing-the-multipoint-services-role-in-window-server-vnext-technical-preview.aspx>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
CommunityDays.it

http://en.wikipedia.org/wiki/Windows_MultiPoint_Server
<http://blogs.technet.com/b/multipointserver/>

<http://blogs.technet.com/b/multipointserver/archive/2013/03/07/roundup-of-online-resources-for-windows-multipoint-server-2012.aspx>
<http://blogs.technet.com/b/multipointserver/archive/2013/01/04/windows-multipoint-server-2012-disk-protection.aspx>
<http://blinditandnetworkadmin.blogspot.it/2012/10/windows-multipoint-server-2012-creating.html>

Gestione ruolo MultiPoint Services

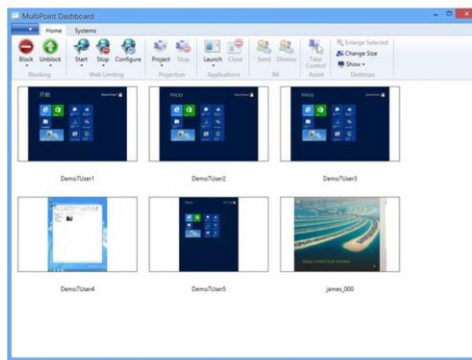
Metodi di deploy

- Dopo il grace period di 180 giorni attivare l'RD Licensing Server tramite l'RD License Manager
- Configurare il licensing per-user e inserire le WMS CALs nel MultiPoint Manager
- Windows MultiPoint Server è indicato per Teachers/students computer labs e Point of sale
- Per la gestione vi sono a disposizione il MultiPoint Manager e la MultiPoint Dashboard

Requisiti Hardware

- Una CPU Dual-core: può gestire fino a 8 stazioni
- Una CPU Quad-core: può gestire fino a 16 stazioni
- Una CPU Quad-core con multithreading: può gestire fino a 20 stazioni
- Una CPU Six-core con multithreading: può gestire fino a 24 stazioni
- Se è necessario utilizzare applicazioni grafiche è raccomandabile disporre di un core per stazione
- E' necessario utilizzare una scheda grafica che consenta di estendere il desktop su più monitor se si utilizza la connessione diretta

<https://technet.microsoft.com/en-us/windows-server-docs/compute/remote-desktop-services/multi-point-services/hardware-requirements-and-performance-recommendations>



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

http://en.wikipedia.org/wiki/Windows_MultiPoint_Server
<http://blogs.technet.com/b/multi-point-server/>

MultiPoint e scenari di configurazione

Multipoint Server singolo in Workgroup

- Creazione di un local user accounts per ogni persona che ha accesso al MultiPoint Server
- Local user accounts creati e gestiti tramite il MultiPoint Manager

Multipoint Server multipli in Workgroup

- Creazione di un local user accounts su ogni MultiPoint Server per ogni persona che accede al MultiPoint Server
- Local user accounts creati e gestiti tramite il MultiPoint Manager su ogni MultiPoint Server

Multipoint Server multipli in Dominio

- Uno o più Multipoint Server membri di dominio
- Utilizzo di domain user accounts gestiti tramite Active Directory (non è possibile usare il MultiPoint Manager)
- Per default gli utenti possono eseguire logon solo su una stazione alla volta (configurazione modificabile tramite il MultiPoint Manager)

Single user account per stazioni multiple

- E' possibile accedere a più stazioni sullo stesso computer contemporaneamente utilizzando un singolo account utente
- Utile in ambienti in cui gli utenti non hanno nomi utente univoci e quindi l'utilizzo di un account utente singolo semplifica la gestione del sistema

FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<https://technet.microsoft.com/en-us/library/jj916410.aspx>

RemoteFX

Ottimizzazione e nuove funzionalità

- Supporto OpenGL 4.4 e OpenCL 1.1 API utili per l'esecuzione delle engineering applications, supporto al codec AVC/H.264
- Dimensione VRAM max per VM può raggiungere un max di 1GB di VRAM dedicata per un totale max di 2GB (1GB dedicata e 1GB condivisa)
- La dimensione della VRAM può essere configurata tramite i cmdlets PowerShell *Add-VMRemoteFX3dVideoAdapter* e *Set-VMRemoteFX3dVideoAdapter*
- Aumento delle performance e bug fixes del canale di comunicazione tra VM e Host basato sul VMBus

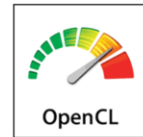
Migliore End User Experience in ambienti VDI per applicazioni Engineering e Designer (per esempio Adobe Photoshop, Maya, Blender e Houdini)

Adobe Photoshop richiede almeno 512MB per abilitare l'accelerazione hardware


Le VM a 32 bits pre W10 non sono in grado di usare più di 512 MB di VRAM dedicata e non eseguono il boot se la VRAM è impostata a 1GB

Limitazioni RemoteFX pre Windows Server 2016

- Nelle precedenti versioni ci si era concentrati sulla End User Experience per migliorare principalmente l'usabilità in RD e VDI di applicazioni Office, web browsing e line of business applications
- Supporto a DX11.1, supporto a OpenGL 1.1 e nessun supporto per OpenCL
- In WS2012R2 la VRAM dedicata max per VM era di 256 MB ed era impostata dinamicamente in base al numero di monitor e alla risoluzione della VM



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<https://technet.microsoft.com/it-it/library/dn765476.aspx?f=255&MSPPError=-2147217396>

<http://blogs.msdn.com/b/rds/archive/2014/11/05/remotefx-vgpu-updates-in-windows-server-next.aspx>

<http://blogs.msdn.com/b/rds/archive/2014/10/07/what-s-new-in-remote-desktop-services-for-the-next-version-of-windows-server.aspx>

<https://blogs.technet.microsoft.com/enterprisemobility/2016/01/11/remote-desktop-protocol-rdp-10-avch-264-improvements-in-windows-10-and-windows-server-2016-technical-preview/>

RD SH e utilizzo di RemoteFx e GPU

Windows Server 2008 R2 SP1

- RemoteFX vGPU e RemoteFX USB redirection supportate solo in VDI
- RD SH supporta RemoteFX advanced bitmap acceleration con l'esclusione delle RemoteApp
- RD SH virtuali possono usare DirectX

RD SH non usa la GPU

Windows Server 2012/R2

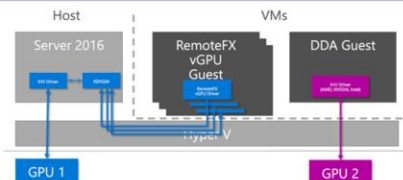
- Le RemoteApp supportano RemoteFX
- RemoteFX USB redirection supportata anche in RD SH
- Policy *Use the hardware default graphics adapter for all Remote Desktop Services sessions* per l'utilizzo dell'hardware graphics renderer della GPU di default anziché il Microsoft Basic Render Driver
- RemoteFX vGPU non supportata in RD SH e RemoteApp

RD SH fisici usano la GPU

Windows Server 2016

- Discrete Device Assignment assegna una GPU ad una VM tramite driver nativo consentendo di utilizzare la policy *Use the hardware default graphics adapter for all Remote Desktop Services sessions*
- RemoteFX vGPU non supportata in RD SH e RemoteApp
- DDA consente l'utilizzo di RemoteFX Adaptive Graphics, RemoteFX for WAN e RemoteFX Media Redirection

RD SH usa la GPU



<http://www.devadmin.it/2016/10/01/remote-desktop-session-host-remotefx-gpu-e-novit-in-windows-server-2016/>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
CommunityDays.it

<https://blogs.technet.microsoft.com/enterprisemobility/2011/03/25/qa-microsoft-remotefx-and-remote-desktop-session-host-servers/>
<https://blogs.technet.microsoft.com/enterprisemobility/2012/09/11/remotefx-usb-redirection-in-windows-server-2012-and-windows-8/>
<https://blogs.technet.microsoft.com/enterprisemobility/2014/06/06/understanding-and-evaluating-remotefx-vgpu-on-windows-server-2012-r2/>
<http://windowsitpro.com/windows-server-2016/when-gpu-can-be-utilized-session-virtualization-2016>
<https://social.technet.microsoft.com/Forums/office/en-US/d91ca694-da27-4273-b225-f5474791bd6c/wms2012-rdsh-does-a-gpu-in-the-host-really-help-for-graphics-performance?forum=windowsmultipointserver>
<https://blogs.technet.microsoft.com/heyscriptingguy/2016/07/14/passing-through-devices-to-hyper-v-vm-by-using-discrete-device-assignment/>

Nuovo modello di deploy

Server Based Personal Session Desktops

- Combinazione delle due modalità Virtual machine-based desktop deployment e Session-based desktop deployment
- Permette di realizzare un VDI tramite un OS server anziché un OS client e quindi di realizzare un'infrastruttura VDI in Azure
- WS2016 ha migliorato la Desktop Experience feature per ottenere il look & feel like di un client Windows 10
- Il deploy e la gestione è possibile tramite PowerShell

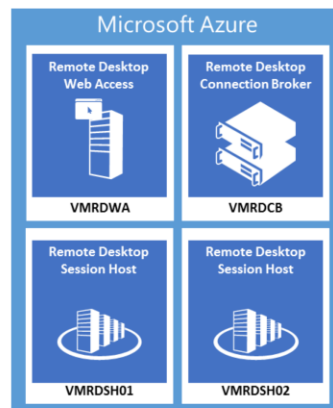
Creazione di una Server Based Personal Session Desktops

```
New-RDSessionCollection -CollectionName ServerBasedPersonal  
-ConnectionBroker VMRDCB -SessionHost VMRDSH01,VMRDSH02  
-PersonalUnmanaged -GrantAdministrativePrivilege
```

Nuova opzione

Assegna diritti di local
administration sul
personal Session Host

<http://www.devadmin.it/2015/06/11/server-based-personal-session-desktops/>



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

<https://technet.microsoft.com/en-us/library/jj215451.aspx>

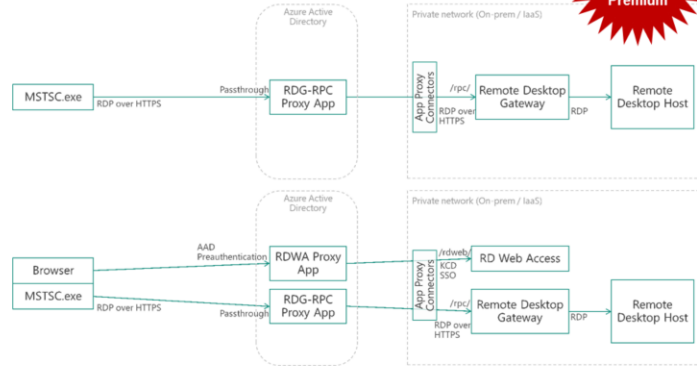
Azure Active Directory App Proxy

Caso 1: AADAP e RD GW

I client si connettono via HTTPS ad AASAP che poi si connette all'RD GW in questo modo l'RD GW non è esposto in Internet

Caso 2: AADAP e RD WA

I client si connettono via AASAP che gestisce pre autenticazione e single-sign-on (SSO) su Azure AD, è però necessaria l'autenticazione sul canale RDP se RD WA usa Kerberos oppure è possibile usare RD WA con Form Authentication senza preautenticazione su Azure AD



AADAP risolve problemi di connettività e garantisce una protezione di base mediante network buffering, hardened Internet frontend e DDoS protection

<https://blogs.technet.microsoft.com/applicationproxyblog/2015/10/14/publishing-remote-desktop-with-azure-active-directory-application-proxy/>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

<https://technet.microsoft.com/en-us/windows-server-docs/compute/remote-desktop-services/desktop-hosting-logical-architecture>

Ulteriori novità

User Experience

- Pen Remoting Support
- Supporto a risoluzioni fino a 4k
- Nuova funzionalità di zoom in MSTSC
- Miglioramenti al Windows client desktop UX



Scalabilità e HA dell'RD Connection Broker

- Supporto alla SQL Authentication
- Supporto a 10k connessioni concorrenti
- Supporto ad Azure SQL Database che permette HA, DR e meccanismi di upgrade

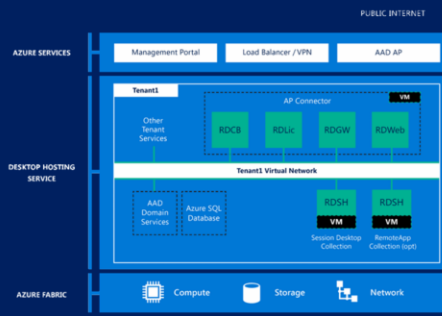


Altri miglioramenti

- Supporto alle VM Gen 2 per il VDI

Architettura ottimizzata per il cloud

- Una VM per RDCB, RDLic, RDGW e RDWeb
- Infrastruttura completa con sole 3 VM



FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 CommunityDays.it

<https://technet.microsoft.com/en-us/windows-server-docs/compute/remote-desktop-services/use-an-azure-sql-database-to-enable-high-availability-for-your-connection-broker>

<https://blogs.technet.microsoft.com/enterprisemobility/2016/05/26/remote-desktop-for-windows-10-exiting-preview/>

<https://blogs.technet.microsoft.com/ausoemteam/2016/09/05/whats-new-in-windows-server-2016-standard-edition-part-10-remote-desktop-services/>

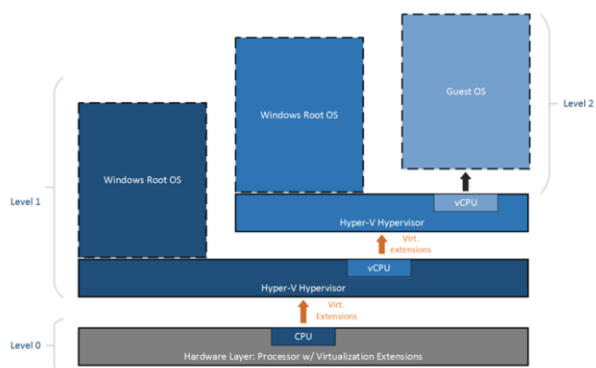
Nested virtualization

Requisiti

- Host Hyper-V WS2016
- VM Hyper-V WS2016 e configuration version 8.0 o superiore
- Intel processor con VT-x e EPT
- Deve essere abilitata sulla VM tramite PowerShell con il cmdlet Set-VMProcessor

Limitazioni

- Dynamic memory non supportata
- Al momento non supportata in Azure
- RemoteFx non è disponibile



Consente la virtualizzazione del ruolo RD Virtualization Host, ma al momento non è possibile eseguire una VM RD VH in Azure

https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/user_guide/nesting

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
CommunityDays.it

<https://technet.microsoft.com/en-us/windows-server-docs/compute/hyper-v/deploy/upgrade-virtual-machine-version-in-hyper-v-on-windows-or-windows-server>

<https://blogs.msdn.microsoft.com/italy/2016/05/30/guest-post-eseguire-lemulatore-di-windows-10-mobile-allinterno-di-una-virtual-machine-con-hyper-v/>

<https://social.msdn.microsoft.com/Forums/en-US/ee654842-5007-4456-96ab-a682ec18591d/nested-virtualization-inside-azure?forum=WAVirtualMachinesforWindows>

<https://blogs.technet.microsoft.com/virtualization/2015/10/13/windows-insider-preview-nested-virtualization/>

<https://lenovopress.com/lp0087.pdf>

A nighttime photograph of a city street, likely in Hong Kong, featuring tall skyscrapers and a multi-lane highway with long-exposure light trails from vehicles. The image is split vertically, with the left side showing a more static view of the buildings and the right side showing the dynamic light trails.

DEMO

Server Based Personal Session Desktops
e ruolo MultiPoint Services

www.futuredecoded.it

 #FutureDecoded

A nighttime cityscape featuring a prominent skyscraper with a blue glass facade and many lit windows. In the foreground, a multi-lane highway shows long-exposure light trails from cars, with red and white streaks indicating traffic flow. A pedestrian bridge with a glass railing is visible above the highway. The overall scene is illuminated by city lights, creating a vibrant urban atmosphere.

RDS Security e Troubleshooting

Remote Desktop Services
stato dell'arte e novità in
Windows Server 2016 e Azure

www.futuredecoded.it



#FutureDecoded

RDS security stack e mitigations

Firewall

Brute Force



Non pubblicare direttamente la porta TCP 3389
Utilizzare RD WA+RD GW, o VPN, o PAT
Disabilitare l'accesso nelle fasce orarie in cui non serve

RD Session Host

DoS



Installare gli aggiornamenti, eseguire BPA regolarmente
Utilizzare NLA
Password Administrator sicura, rename Administrator

Sessione Utente

Ramsonware



Se possibile pubblicare solo RemoteApp e non il desktop
Bloccare con GPO funzionalità non pertinenti
Bloccare redirezioni non utilizzate

Credenziali Utente

Ramsonware



Password complesse, Two-factor authentication
Nomi account non individuabili con attacchi a dizionario
GPO blocco account, GPO autorizzazione logon su RDS

Privilegi Utente


Ramsonware



Privilegi minimi su server RDS
Privilegi minimi sulle risorse dell'infrastruttura

<http://www.devadmin.it/2013/10/08/hardening-di-un-server-remote-desktop/>

FUTURE | **MILANO**
DECODED | OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<https://security.berkeley.edu/resources/best-practices-how-articles/securing-remote-desktop-rdp-system-administrators>

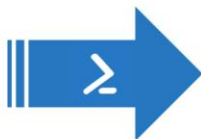
Monitoraggio accessi via PowerShell

Get-EventLog

- **Accesso riuscito:** Security event 4624
- **Accesso fallito:** Security event 4625
- Estrapolazione informazioni specifiche dell'evento tramite array **ReplacementStrings**

Send-MailMessage

Invio mail contenente report del controllo eventi per individuare accessi non autorizzati e attacchi brute force



Da:	[REDACTED]
A:	[REDACTED]
Cc:	[REDACTED]
Oggetto:	Attenzione: 1 accesso amministrativo è stato fallito negli ultimi 30 minuti
Accessi con account Administrator:	
10/10/2013 17:01:49	da IP: [REDACTED]
Tentativi di accesso con credenziali errate:	
10/10/2013 17:11:09	da IP: [REDACTED] Utente: admin
10/10/2013 17:11:07	da IP: [REDACTED] Utente: admin
10/10/2013 17:11:04	da IP: [REDACTED] Utente: admin
10/10/2013 17:06:07	da IP: [REDACTED] Utente: [REDACTED]
10/10/2013 17:02:51	da IP: [REDACTED] Utente: Administrator
10/10/2013 17:02:51	da IP: [REDACTED] Utente: Administrator
10/10/2013 17:01:42	da IP: [REDACTED] Utente: Administrator
10/10/2013 17:01:37	da IP: [REDACTED] Utente: Administrator

<http://www.devadmin.it/2013/10/10/monitoraggio-degli-accessi-tramite-powershell/>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

RDS BPA e RDS Diagnostic Tool

RDS Best Practices Analyzer (RDS BPA)

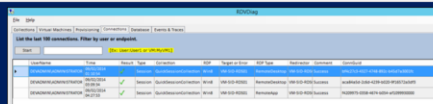
- Aggiornabile tramite WSUS
- Eseguito periodicamente permette di prevenire eventuali issue
- Automatizzabile tramite PowerShell

```
Get-BPAModel  
Invoke-BPAModel  
Get-BPAResult  
Set-BPAResult
```




RDS Diagnostic Tool

- Scaricabile dal Microsoft Download Center
- Supporta WS2012 e WS2012 R2
- Deve essere avviato sull'RD CB
- Deve essere eseguito con un account avente privilegi amministrativi su tutti i server dell'infrastruttura RDS



<http://blogs.msdn.com/b/rds/archive/2013/11/04/remote-desktop-services-diagnostic-tool.aspx>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

<http://www.virtualizationadmin.com/articles-tutorials/general-virtualization-articles/troubleshooting-rds-windows-server-2012.html>

Tools Microsoft e di terze parti

Remote Desktop Connection Manager 2.7

- Gestione di multi connessioni RD per W8/8.1 WS2012/R2
- Supporto a Virtual machine connect-to-console
- Smart groups
- Supporto per credential encryption tramite certificati
- Scaricabile dal Microsoft Download Center



LazyTS

- PowerShell script per gestire Sessioni e Processi locali o remoti
- Scaricabile da GitHub o TechNet Gallery (<http://www.lazywinadmin.com/p/lazyts.html>)



User Profile Cleaner

- Rimozione profili utente inutilizzati
- Utility GUI o command line per la rimozione dei profili utente non utilizzati da un determinato numero di giorni con possibilità di definire una lista di esclusione
- Scaricabile da CodePlex (<https://upcleaner.codeplex.com/>)



<https://blogs.technet.microsoft.com/rmilne/2014/11/19/remote-desktop-connection-manager-download-rdcman-2-7/>

**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

Hotfixes e updates

Recommended hotfixes and updates for Remote Desktop Services in Windows Server 2012 R2
<https://support.microsoft.com/en-us/kb/3147099>



Available Updates for Remote Desktop Services in Windows Server 2012 R2
<https://support.microsoft.com/en-us/kb/2933664>




Available updates for Remote Desktop Services in Windows Server 2012
<https://support.microsoft.com/en-us/kb/2821526>



Available Updates for Remote Desktop Services (Terminal Services) on Windows Server 2008 R2 SP1
<https://support.microsoft.com/en-us/kb/2601888>



**FUTURE
DECODED** | **MILANO**
OCT 6-7 / 2016

In partnership with:
 **CommunityDays.it**

A nighttime cityscape featuring a highway with long-exposure light trails from cars. In the background, several tall skyscrapers are illuminated, including the Burj Khalifa. A pedestrian bridge with a pink railing is visible in the foreground on the right.

DEMO

Monitoraggio accessi RDS
e RDS Diagnostic Tool

www.futuredecoded.it

 #FutureDecoded

