EiS
Andrea Varavallo
20/lug/2014

# Preparazione clients SSBAR

## Software da installare, servizi, configurazione

L'analisi dei computer da destinare all'utenza preparati pochi giorni addietro rispetto al momento della stesura di questo documento ha evidenziato diverse e diffuse pecche soprattutto per quanto concerne l'utilizzo improprio dell'accesso a internet e dell'inutile profluvio di software opzionale e non lavorativo installato mediante i meccanismi del windows update. Nelle pagine successive troverete una serie di check list da utilizzare come sistema di controllo della qualità relativamente ai PC da consegnare, di modo che le operazioni compiute sui client vadano, nei limiti del possibile e dell'applicabile, a costituire un nucleo di automatismi lavorativi. Attualmente troppo è lasciato alla fantasia del singolo e sappiamo come tale comportamento ha "danneggiato" l'utilizzabilità delle varie LAN operative nella nostra organizzazione.

Vale comunque la raccomandazione generale di limitarsi al solo software correttamente licenziato: sottolineo qui, se ce ne fosse ancora bisogno, che non abbiamo la disponibilità delle licenze di WinZip, di Nero Burning Rom (e di altro ancora che adesso non mi sovviene) e che va spiegato all'utente che le funzionalità offerte da questi software sono ormai nativamente disponibili nel S.O. (al massimo potrete erogare una piccolissima sessione di formazione, così come è capitato recentemente a me e Gianluca a Palazzo Altemps dove è stato mostrato a un utente dotato di XP come masterizzare ricorrendo a quanto il sistema operativo già offre da diversi anni). A Palazzo Massimo è attivo il sistema WSUS (server 10.1.4.243) in grado di provvedere agli aggiornamenti più importanti per le macchine inserite nelle opportune "Unità Organizzative" di Active Directory.

Spero contribuirete a questo documento con idee e modifiche per renderlo davvero utile in quella che è l'attività quotidiana del gruppo di help-desk: prendete queste quattro righe però cum grano salis, siate elastici dove è necessario e mantenete la barra a dritta ove non sono utili voli pindarici in termini di configurazione e software da destinare all'utenza.

# Client Palazzo Massimo

**Software da installare e configurare (sostrato comune)**

• Windows updates: limitarsi alla sola categoria comprendente le patch di sicurezza per exploit noti e a quanto obbligatorio/fondamentale; tralasciate senza problemi tutto il software opzionale;

• Microsoft Office: deve essere eseguita un'installazione personalizzata e limitata ai soli Word, Excel, Access, Power Point; la lingua del sistema di aiuto integrato in questi programmi deve essere l'italiano;

• Non installate la patch "Microsoft Office file validation Add-In";

• Acrobat Reader nell'ultima release disponibile con la disattivazione dei meccanismi di aggiornamento automatico;

• Mozilla Firefox con disattivazione dei meccanismi di aggiornamento automatico del programma core e delle estensioni/plugin;

• Mozilla Thunderbird con disattivazione dei meccanismi di aggiornamento automatico del programma core e delle estensioni/plugin;

• Open Office: disattivare le funzionalità di aggiornamento

• Software Adobe (Photoshop etc.): disattivare le funzionalità di aggiornamento automatico;

• Software HP (scanner, stampanti): disattivare le funzionalità di aggiornamento automatico;

• Google Chrome: disattivare le funzionalità di aggiornamento automatico e le funzioni di prefetching per il miglioramento delle prestazioni;

• Plugin flash per i browsers;

• Viewer free di Autocad (se disponibile/individuato); tale software non è strettamente indispensabile in quanto AutoDesk fornisce i servizi cloud a nome "360.autodesk.com" dove, previo accredito (o utilizzo di quanto già in possesso come account di G+, Facebook o altri social network) è possibile caricare i files da visualizzare - va da sé che tale tipologia di soluzione prevede necessariamente un collegamento a internet;

• Non installate Microsoft Silverlight se non per esplicita necessità (ad esempio, sarà indispensabile per poter controllare le telecamere di Villa Dei Quintili sulla macchina della Paris);

• Non installate i packages Windows Live;

• Antivirus MS o Avira per i client XP oramai fuori assistenza; su Avira è indispensabile confrontarci in quanto ho notato installazioni effettuate alla carlona;

• Java Runtime Environment: non abbiamo software lavorativi che richiedono l'utilizzo della JVM Oracle, quindi non installatela a meno di esigenze specifiche e comunque le funzionalità di aggiornamento automatico devono essere disattivate;

• Non installate software di supporto allo streaming audio/video a meno di specifiche e comunicate esigenze LAVORATIVE;

• Non installate software di comunicazione personale, a meno di specifiche e comunicate esigenze LAVORATIVE;

• Quando si cambiano le stampanti, soprattutto se si passa a produttori differenti, il software precedente deve essere rimosso (sembra ridondante segnalare tale evenienza ma, nei fatti, tale regola di puro buon senso non è punto seguita);

• L'installazione del software HP di gestione di scanner e stampanti deve essere limitata allo stretto necessario, senza caricare le macchine di quanto accessorio o opzionale presente nei packages HP;

**Servizi**

• Disattivare il servizio di aggiornamento del plugin Flash;

• Disattivare il servizio di aggiornamento di Adobe Acrobat Reader:

• Controllare che sia attivo il servizio di aggiornamento mediante Windows Update;

• Disattivate i servizi (e disinstallate dove tale azione è appropriata) che utilizzano impropriamente le risorse di rete (Apple Bonjour, Google Update Helper, i servizi Apple Mobile, iTunes, Samsung Kies, Nokia);

**Configurazione**

Da diverso tempo la configurazione delle variabili TCP/IP è automatica sulle reti principali della SSBAR: il DHCP è in funzione sui firewall locali e sul server Augusto (10.1.4.245) di Palazzo Massimo. Nessuna azione è richiesta da parte vostra. Da Gennaio a Palazzo Massimo è attiva la configurazione automatica delle impostazioni proxy sia come policy computer che come utente per le macchine correttamente in dominio e gli oggetti "user" di Active Directory. Gli scripts funzionano per Windows XP, Windows 7 e Windows 8 e Windows 8.1. Tali piccoli programmi si occupano di impostare i proxy per il sistema operativo e per il browser. Condizione necessaria e sufficiente è che la macchina sia correttamente inserita nel dominio. Le policies sono applicate, a partire dai server centrali,

ogni 90 minuti. Nel caso in cui gli automatismi non dovessero entrare in funzione al fine di avere l'accesso a internet mediante browser è necessario far riferimento al file di configurazione del proxy, la cui url è "http://intranet.sar.it/proxy.pac". Tale file contiene già le necessarie direttive di esclusione di utilizzo del proxy per, ad esempio, l'accesso al protocollo di modo che non debbano essere inserite a mano. Per l'accesso a internet da riga di comando, variabile a seconda del sistema operativo utilizzato e già mostrata in precedenti riunioni del servizio di helpdesk, si può puntare all'indirizzo resistente del firewall, vale a dire 10.1.4.1 porta 3128. La lista di quanto deve essere controllato sui PC:

- Accesso e gestione RPC a sezione utenze e gruppi locali, servizi;
- Accesso e gestione RPC del registro di sistema del client;
- Accesso e gestione RPC al catalogo degli eventi del client;
- Appartenenza dell'utente che userà la macchina al gruppo che consente l'accesso in RDP;
- Ricezione policies;
- Configurazione eventuali cartelle condivise eventuali mediante uri resistente ("\\sar.it \dati\") ;
- Configurazione e controllo stampanti di rete/locali;
- Configurazione e controllo scanner;
- Configurazione e controllo di funzionamento per eventuali periferiche USB;
- I browser devono avere come pagina predefinita la intranet aziendale: evitare gli accessi inutili e dannosi dal punto di vista della larghezza di banda impiegata alle pagine predefinite di IE, quali MSN, Hotmail etc.;
- Controllo dello "event viewer" del client al fine di individuare le problematiche più importanti;
- Disabilitazione dell'IPV6 (inutilizzato/inutilizzabile sulla rete SSBAR);

## Client Terme di Diocleziano

Le indicazioni relative ai client di Palazzo Massimo vanno prese globalmente in considerazione con l'eccezione rappresentata dal servizio di aggiornamento del software del s.o.: vista la ridotta disponibilità di banda è necessario fermare i meccanismi di "update" e procedere in tal senso sui client quando ve n'è la necessita e l'agio (presto avremo la soluzione, sotto forma di una nuova linea dati o di server aggiuntivi in situ utilizzati per concentrare gli

aggiornamenti). Tenete comunque in considerazione che il server proxy per le Terme di Diocleziano è disponibile all'indirizzo 10.1.6.12, porta 3128.

## Client Palazzo Altemps

Valgono le regole seguite per le Terme di Diocleziano. Il server proxy per questa sede risponde all'indirizzo 10.1.3.1, porta 3128 e viene iniettato direttamente mediante l'url http://intranet.sar.it/proxy.pac

## Client Palatino

Anche in questo caso valgono le regole già viste: il proxy server è la macchina 10.1.2.1, porta 3128 e url http://intranet.sar.it/proxy.pac

## Client Ufficio Tecnico di Via Gaeta

Per l'ufficio tecnico di via Gaeta è stata recentemente (fine giugno 2014), previsto un branching nel file "proxy.pac" distribuito dal server intranet.sar.it: è prevista quindi, anche per via Gaeta, la distribuzione della regola di configurazione automatica del proxy server per i client correttamente in dominio. Tale branching non fa altro che restituire al browser che tenta l'accesso a internet, la direttiva "DIRECT" in quanto non abbiamo (ancora) un proxy server in situ. Per la preparazione fine dei clients bisogna fare riferimento a quanto già riportato in questo documento per la sede di Palazzo Massimo.

## Client Villa di Capo di Bove

Tale sede è fisicamente "bridged" mediante un ponte radio a Palazzo Massimo e non è chiaro il perché della scelta di non inserire in dominio i client, sia per l'evidente vantaggio di configurabilità ed accessibilità remota che per i ridotti tempi di intervento che ne conseguono. L'unico svantaggio visibile in lontananza può avere a che fare con l'instabilità del ponte stesso (il sistema di controllo Nagios segnala comunque uno stato "up" per il 98,468% del tempo dal primo gennaio 2014 alla data di questo documento), fattore risibile rispetto ai vantaggi elencati. Una nuova configurazione di Squid è stata messa in pratica (direttiva "http_port 10.1.13.252:3128") e l'accesso a tale indirizzo viene automaticamente gestito dal proxy.pac iniettato automaticamente nelle macchine correttamente posizionate nel dominio "sar.it".

Nelle ultime due settimane la totalità dei client in situ è stata spostata nel dominio succitato. I clients vanno preparati secondo le direttive previste per le macchine di Palazzo Massimo.

## Note generali

In questi mesi di lavoro si è avuto modo di notare alcune differenze di comportamento relativamente alle capacità dei browsers di utilizzare ed effettuare un parsing corretto del file proxy.pac. Il software Mozilla Firefox con versione 13 (non abbiamo avuto tempo e modo di sperimentare più numeri di versione) non lavora bene con lo script js in questione: basta un aggiornamento all'ultima versione per eliminare i problemi di collegamento ai siti esterni. Discorso similare vale per Internet Explorer 10 che spesso genera immediatamente un errore di accesso alla rete all'apertura: basta aggiornare all'ultima versione disponibile. In alcune sedi (Terme di Diocleziano, Palazzo Altemps e al Palatino - per tamponare l'emergenza di utilizzo della banda internet disponibile) per portare a termine gli aggiornamenti deve essere modificata l'area "FORBIDDEN" del plugin SquidGuard.

**VADEMECUM comandi di utilità:**

- aggiornamento forzato delle policies di dominio: "***gpupdate /force***";
- visualizzazione delle policies attive ed ereditate: "***gpresult /r***";
- accesso remoto a macchina di dominio: "***psexec.exe \\nome-computer -accepteula -u sar \utente_amministrativo_dominio -p password_utente_amministrattivo_dominio CMD***";
- visualizzazione da remoto del software installato una volta entrati sul client come al punto precedente: "***wmic /node:localhost product get name,vendor < NUL:***";
- rimozione silente e senza interazione da parte utente di software una volta entrati sul client: "***wmic /node:localhost product where name="nome_software" call uninstall /nointeractive < NUL:***";
- rimozione silente e senza interazione da parte utente utilizzando wildcard:
  - ***wmic /node:localhost product where "name like '%live%' " call uninstall /nointeractive***
- Proxy pac: "http://intranet.sar.it/proxy.pac";
- Ridenominazione remota delle macchine: "***netdom renamecomputer \\nome_computer \NewName:nuovo_nome \UD:sar\utente_amministrativo_dominio \PD:password_utente_amministrativo_dominio /REB /FORCE***";
- Impostazione proxy server per S.O. Win7/8/8.1: "***netsh winhttp set proxy ip:port***";
- Impostazione proxy server per S.O. WinXP: "***proxycfg -p ip:port***";
- Visualizzazione dei processi in esecuzione su un pc: "***wmic /node:localhost process get name < NUL:***";
- Spegnimento forzato di un processo problematico: "***wmic /node:localhost process where name ='nome_processo' delete < NUL:***"
- Passaggio a dhcp: ***netsh interface ip set address "Connessione alla rete locale (LAN)" dhcp***