
SERVIZIO DI ADEGUAMENTO DELLA INFRASTRUTTURA INFORMATICA DEI DIPARTIMENTI ARPAM DI ANCONA E MACERATA

Specifiche tecniche

Il presente documento disciplina le specifiche tecniche del servizio relativo all'adeguamento della infrastruttura informatica dei Dipartimenti di Ancona e Macerata dell'Agenzia Regionale per la Protezione Ambientale Marche, di seguito ARPAM.

1) Sommario

1) Sommario	1
2) Descrizione dell'architettura informatica ARPAM	1
a) Dipartimento di Ancona (Ancona, via Colombo, 106)	2
b) Dipartimento di Macerata (Macerata, via Federico II, 41)	2
3) Specifiche dell'adeguamento	3
a) Lavori generici lato server	3
b) Lavori generici lato client	4
c) Lavori generici di networking	5
d) Lavori specifici dipartimento di Ancona	5
e) Lavori specifici dipartimento di Macerata	5
4) Configurazioni di backup	6
5) Formazione	7
6) Modalità di intervento	7
7) Condizioni di affidabilità	8

2) Descrizione dell'architettura informatica ARPAM

I servizi informatici dell'ARPAM sono dislocati su 7 (sette) sedi territoriali, 5 (cinque) di queste sedi sono consolidate in un dominio unico Microsoft con functional level WS2012 e non sono oggetto di intervento; le sedi di Ancona (AN) e Macerata (MC) sono tutt'ora organizzate in domini Microsoft separati con functional level WS2003 e costituiscono le uniche sedi di intervento del presente affidamento, che prevede il loro rinnovo e la loro unificazione a dominio unico con l'utilizzo di un DFS centralizzato nella sede regionale.

Per le due sedi in oggetto si forniscono le caratteristiche allo stato attuale e, di seguito, le caratteristiche che dovranno risultare al termine degli interventi richiesti al fornitore.

a) Dipartimento di Ancona (Ancona, via Colombo, 106)

La sede del dipartimento di Ancona è organizzata su 3 (tre) palazzine, due delle quali sono a tre piani, una su piano singolo. Tutte le palazzine sono dotate di uno o più rack ed uno o più switch. Sulla palazzina principale sono attestate le linee di arrivo in fibra. In tutto sono presenti 6 (sei) switch di cui 5 (cinque) sono da sostituire. Tutte le dorsali sono in fibra.

Lo stato del dominio è il seguente:

- Dominio autonomo WS2003;
- n.5 server fisici, di cui 2 sono oggetto di intervento;
- n.1 NAS TS451 4x3Tb in RAID5 QNAP,
- sistema di backup a nastro (da dismettere) con software BackupExec;
- circa n.55 Personal Computer fisici, di questi circa 15 con sistema operativo XP e circa 25 con sistema operativo windows Seven, gli altri in windows 10;
- circa n.30 PC/notebook nuovi a sostituzione di altrettanti PC preesistenti;
- n.6 switch hp/cisco con n.2 media converter fibra/rame;

Caratteristiche richieste a termine intervento sono:

- dominio unificato ARPAM;
- n.1 host fisico di virtualizzazione;
- n.2 VM ws2019 in MS HYPER-V;
- n.1 NAS TS451 4x3Tb RAID5 QNAP;
- circa n.55 PC/notebook in dominio unificato, tutti con sistema operativo windows 10;
- sistema di backup VEEAM su QNAP;
- n.6 switch cisco 2960 48p in gbic

b) Dipartimento di Macerata (Macerata, via Federico II, 41)

La sede del dipartimento di Macerata organizzata su due piani con due armadi rete connessi tramite cablatura in rame categoria 6, in un armadio sono attestate le linee di arrivo in fibra. In tutto sono presenti 6 switch (4 in stack), tutti da sostituire.

Lo stato del dominio è il seguente:

- Dominio autonomo WS2003;
- n.2 server fisici;
- n.1 Servizio di terminal server su WS2008;
- n.1 NAS QNAP TS420 da 3x3tb in raid5;
- circa n.40 Personal Computer fisici con erogazione servizi in terminal server;
- circa n.25 PC/notebook nuovi a sostituzione di altrettanti PC preesistenti;
- n.4 switch 3com in stack, n.2 switch HP;

Caratteristiche richieste a termine intervento:

- Dominio unificato ARPAM
- n.1 host fisico di virtualizzazione
- n.2 VM ws2019 in MS HYPER-V;
- n.1 NAS QNAP TS420 da 3x3tb in raid5,
- Rimozione servizi di terminal server;
- Circa n.40 PC/notebook in dominio unificato, tutti con sistema operativo windows10;
- Sistema di backup VEEAM su QNAP;

- n.3 switch cisco 2960x 48p, due al piano terra, uno al primo piano.

Per ogni sede è presente un server fisico MS WS2008 in rete di connessioni interdipartimentali su host fisico IBM x3400/x3500 M3/M4. Questi server costituiscono una rete dati con database MS-SQL in replica. Questi server non sono oggetto di intervento organico. Su essi occorrerà comunque lavorare per:

- collocazione nel nuovo dominio unificato ARPAM;
- per il solo server IBM di Macerata, dismissione sistema Terminal Server con rimozione servizi e conseguente migrazione e pulizia dei dati.

In ogni dipartimento esistono circa 2 stampanti di corridoio per piano collegate in rete, a noleggio, di marca Kyocera o Samsung; queste stampanti sono oggetto di configurazione del printer server locali.

3) Specifiche dell'adeguamento

Il fornitore dovrà eseguire installazioni e configurazioni informatiche secondo quanto riconosciuto come *best practice*, che riguardano sia sistemi operativi server, sia sistemi operativi client, apparati di rete, cablatura minima ove necessario, in entrambe le sedi oggetto dell'appalto, in base alle descrizioni generiche e specifiche dei singoli dipartimenti come nel seguito indicato.

a) Interventi generici lato server

Nei due dipartimenti interessati dall'affidamento sono già stati installati, acquistati e messi in esercizio provvisorio due server nuovi (uno per dipartimento) con le seguenti caratteristiche:

- HP Proliant DL560g10;
- Doppio processore Xeon Gold 5218;
- 128 gb RAM;
- 2 HD 300gb mirroring per Sistema operativo, 4 HD 1.2TB per dati in RAID5;
- Licenza base a aggiuntiva MS WS2019;
- User Call.

I server sono attualmente accessi e collaudati, presenti in test nel dominio unificato ARPAM e non svolgono servizio effettivo.

Le prestazioni oggetto dell'affidamento prevedono, per ogni dipartimento:

- la dismissione dei server di dominio locale;
- la dismissione del dominio Microsoft ADDS locale;
- breve verifica di funzionalità dei nuovi server (già collaudati in fornitura);
- la reinstallazione dei sistemi operativi con la creazione di un virtualizzatore Microsoft HYPER-V e due server virtuali WS2019;
- il promoting del nuovo Domain Controller a dominio unico arpam;
- la configurazione e la verifica di tutti i servizi di dominio replicati;
- la creazione dei nuovi account utenti dipartimentali con l'eventuale integrazione di quelli già esistenti. L'attività prevede anche la normalizzazione e la riorganizzazione del sistema degli account locali che, al termine del servizio, dovrà essere resa omogenea con il dominio ARPAM comprendente tutte le sedi;
- la gestione degli oggetti ADDS (risorse, servizi, utenti);
- la creazione dei gruppi, delle UO e delle GPO di base per il dipartimento nel dominio unificato e la verifica delle attività di sincronizzazione nel dominio unico.

Al termine del servizio i due server virtuali creati per ogni dipartimento dovranno risultare così separati e predisposti:

- Domain Controller: con funzioni DC, DNS, DHCP, GPO ed ogni altro servizio base di ADDS;
- Server di dominio: con funzioni WSUS, Printer Server, File server, DFS;
- Funzione di backup VEEAM su QNAP come indicato in seguito.

Per quanto attiene ai servizi WSUS, ARPAM sta attrezzando un WSUS di upstreaming nella sede collocata in Regione Marche. Il fornitore dovrà configurare i WSUS locali come piattaforme in downstream agganciandosi ai servizi principali preesistenti. Qualora il servizio di upstreaming non fosse ancora stato predisposto, il fornitore configurerà in maniera indipendente i servizi di WSUS dipartimentali predisponendo quanto necessario per l'aggancio al server upstreaming.

Per quanto attinente alle architetture File Server, dovrà essere configurato il servizio DFS da concordarsi con i tecnici ARPAM ed in sincronia con l'attuale DFS presente nella sede regionale. Per i servizi di file server, a titolo di esempio, dovranno essere predisposte le funzionalità ACL, i sistemi di quote di spazio riservato, l'organizzazione delle cartelle e degli sharing secondo gruppi e policy predisposti da ARPAM in relazione con i gruppi di dominio unico, le mappature automatiche delle cartelle di rete per account e le opportune policy degli accessi.

Procedure analoghe devono essere implementate per quanto attinente il sistema di printer server, con relativa configurazione delle stampanti condivise tramite policy e diritti di accesso.

b) Interventi generici lato client

Con l'istituzione del dominio unico e con la dismissione del terminal server ove presente (sede di Macerata), si rende necessario l'inserimento di tutti i PC/notebook locali nella nuova infrastruttura e nel nuovo dominio unico.

I client locali sono forniti di sistema operativo MS Windows 7 pro o successivi. Esistono alcuni client locali con sistema operativo windows XP che sono integralmente da sostituire con i nuovi PC/notebook windows 10 pro contestualmente alla migrazione di dominio.

Si distinguono tre tipologie di intervento sui client locali:

- client w10pro: migrazione diretta del client esistente. In tal caso si richiede la verifica del funzionamento sul nuovo profilo account e sul nuovo dominio del software e delle configurazioni presenti in precedenza;
- client w7pro con hardware adeguato: aggiornamento di un client win7pro al sistema operativo win10pro e migrazione a dominio unico. Come nel punto precedente si richiede la verifica del completo funzionamento sul nuovo sistema operativo e sul nuovo profilo account di quanto prima in esercizio;
- client winXP o w7pro con hardware non adeguato: dismissione del client esistente e messa in esercizio del nuovo PC/notebook sostitutivo con sistema operativo win10pro. In tal caso si richiede anche l'installazione dei comuni software aziendali (a titolo di esempio minimo: pacchetti office automation, lettore PDF, decompressori, antivirus aziendale, software di firma, java, browser alternativo, tool helpdesk remoto, collegamenti al sistema di protocollo e ai gestionali aziendali via web, verifica funzionalità connessioni stampanti via GPO).

In tutti i casi è a carico del fornitore la migrazione completa delle piattaforme client e dei profili utenti come sopra indicato. I tecnici ARPAM forniranno una checklist del software da installare/verificare specificando quanto sopra indicato.

La migrazione dovrà includere tutte le caratteristiche del profilo, i documenti, le ACL per le cartelle di rete e locali, il client di posta ed ogni dato o informazione venga richiesta dal titolare del profilo del vecchio dominio che sarà presente per verificarne le funzionalità complete.

È consentito utilizzare tool automatizzati purché alla migrazione automatizzata segua verifica e integrazione delle informazioni eventualmente mancanti.

In entrambi i dipartimenti sono presenti PC in accoppiamento agli strumenti di analisi. In genere questi PC pilota non sono connessi alla rete aziendale e non sono oggetto di aggiornamento/migrazione. Tuttavia, qualora fossero in rete aziendale, nella configurazione del nuovo servizio DHCP, i loro indirizzi di rete fissi devono essere rilevati ed esclusi dal range di rilascio.

Tutte le licenze software sono a carico ARPAM.

c) Interventi generici di networking

Per ogni dipartimento è necessario rinnovare gli switch presenti negli armadi di piano, obsoleti e di produttori eterogenei.

ARPAM ha preventivamente acquisito n.9 switch Cisco C29060X-48TD-LC con 9 gbic a corredo, altri gbic sono a disposizione qualora necessario.

Gli switch cisco dovranno essere configurati e posti in opera nei rispettivi rack di piano secondo le seguenti configurazioni:

- MC: 2 switch piano terra (eventualmente in stack);
- MC: 1 switch primo piano;
- AN: 2 switch in stack piano primo palazzina A, configurazione da concordarsi con la Regione Marche;
- AN: 3 switch (uno per piano) palazzina B;
- AN: 1 switch palazzina D.

Tutti gli switch di Ancona dovranno essere configurati con cablatura in fibra e gbic sostituendo i media converter ove presenti. Per motivi di porte gbic disponibili ARPAM si riserva la decisione di sostituire uno degli switch Cisco di Ancona palazzina B con un HP 5130 dotato di 4 porte in fibra.

Tutti gli switch vanno configurati con unica VLAN e accesso smart a controllo remoto.

Le configurazioni degli switch vanno impostate in accordo con i tecnici ARPAM, sentiti i tecnici della Regione Marche che devono poter accedere alle configurazioni.

d) Interventi specifici dipartimento di Ancona

Oltre a quanto indicato per interventi generici, per il dipartimento di Ancona si rende necessaria in modo rilevante l'attività di riprogettazione del piano indirizzi IP. In particolare si dovranno effettuare:

- ricognizione, rilevazione degli host e analisi completa del piano di indirizzi IP attuale;
- ridefinizione delle aree in DHCP ed eventuale ricollocazione dei PC con indirizzi fissi;
- ricollocazione quando necessario delle NIC con indirizzi sovrapposti (switch, stampanti).

Le attività di cui sopra possono essere svolte anche con una pre-analisi ed un intervento preventivo da effettuarsi in collaborazione con i tecnici ARPAM prima di procedere all'attività di migrazione, in modo da ottimizzare i tempi e non costituire ulteriore ritardo durante il blocco dei servizi dipartimentali.

e) Interventi specifici dipartimento di Macerata

Il dipartimento di Macerata eroga servizi tramite una architettura terminal server su piattaforma WS2008. Il servizio era prima collocato su uno dei server WS2003 attualmente da

dismettere; per ragioni di efficienza è stato trasferito da qualche anno sulla macchina WS2008 che eroga anche i servizi dei database ambientali.

Il fornitore, per il dipartimento di Macerata, dovrà in specifico:

- Predisporre le attività necessarie per la dismissione del servizio Terminal Server e provvedere alla conseguente salvaguardia e trasmissione integrale dei dati account sul nuovo server virtuale dei servizi;
- Ripulire e ottimizzare il server WS2008 dai contenuti terminal;
- Installare sulle postazioni client i software attualmente utilizzati in configurazione terminal (a titolo di esempio, pacchetti office automation, gestori PDF, decompressori, antivirus aziendale, firma digitale) come indicato nei lavori generici lato client;
- Spostare tutte le configurazioni personalizzate degli account sui nuovi PC/notebook locali o sulle postazioni Personal che ARPAM riterrà essere ancora idonee per supportare un carico di lavoro autonomo;
- Provvedere a ricostruire in ADDS per ogni account un profilo utente locale il più possibile omogeneo con la migrazione del profilo dai servizi Terminal;
- Riconfigurare e migrare le caselle di posta di ogni singolo utente dal terminal. Attualmente su terminal è in uso Microsoft Live Mail e la posta dovrà essere portata in Microsoft Outlook locale senza perdita di mail. La maggior parte dei profili in live Mail sono configurati in POP3.

Tutte le licenze software locali necessarie per attuare la migrazione (ad ex, MS Office) sono a carico di ARPAM.

4) Configurazioni di backup

Nei dipartimenti oggetto dell'affidamento, i sistemi di backup sono al momento parzialmente funzionanti o comunque non efficienti.

Il fornitore dovrà implementare le politiche di backup dipartimentali secondo le best practices sulla scorta dei seguenti principi:

- Il software deve essere installato a scelta sul virtualizzatore MS HYPER-V o sulla VM di servizi, purché abbia accesso ai documenti in file sharing DFS;
- devono essere implementate politiche di backup incrementale/differenziale giornaliero e politiche di backup completo a livello settimanale;
- per i backup completi devono essere adottate politiche di ritenzione sul paradigma GFS (grandfather, father, son) salvo diverse indicazioni da concordarsi con ARPAM in fase dei lavori;
- deve essere possibile attuare backup granulari e di files singoli in caso di necessità;
- deve essere attuato un backup almeno settimanale completo delle macchine virtuali;
- devono essere utilizzati i sistemi QNAP come supporto di backup;
- deve essere utilizzato l'applicativo VEEAM;
- devono essere configurati sistemi di alert e reportistiche automatiche da memorizzare ed inviare in posta elettronica a supervisori di processo.

Si intende che il software necessario alla attuazione di queste politiche e le licenze relative sono a carico di ARPAM.

5) Formazione

Al termine del servizio ed a piena efficienza delle configurazioni attuate, il fornitore si impegna ad impartire una mezza giornata di corso ai tecnici designati da ARPAM in merito a:

- strumenti di controllo e configurazione delle piattaforme HYPER-V. La formazione deve coprire le comuni procedure di controllo sulle macchine virtuali in ambiente HYPER-V come ad esempio la creazione, lo spostamento, lo spegnimento, il riavvio, l'aggiornamento, gli snapshot, i consolidamenti e le modifiche alla configurazione delle risorse delle macchine virtuali create, oltre che alla gestione degli spazi su disco;
- strumenti di controllo e configurazione delle procedure di backup VEEAM. La formazione deve riguardare la schedulazione, la configurazione, la verifica dei processi di backup, l'attuazione delle procedure per il recupero dati;
- connessione, accesso e verifica minima funzionalità switch cisco 2960, anche tramite protocollo HTTPS.

L'attività di formazione deve essere eseguita a servizio concluso.

6) Modalità di intervento

I servizi in oggetto richiedono necessariamente attività in loco. A scopo preparatorio e per ridurre i tempi di inattività dei dipartimenti possono essere attivate procedure di accesso remoto sia prima che dopo le attività territoriali.

Il fornitore dovrà intervenire con proprio personale con almeno 2 (due) tecnici, di cui almeno un tecnico senior certificato (come indicato nelle condizioni di affidabilità), che farà anche da riferimento ed interfaccia con i tecnici ARPAM per l'esecuzione dei lavori. La nomina del tecnico senior certificato può essere differente per i due dipartimenti.

Durante l'esecuzione del servizio, i tecnici ARPAM saranno disponibili per le sole attività di supervisione e consultazione. Per l'esecuzione del servizio, al tecnico senior certificato verrà riconosciuto un account amministrativo nel nuovo dominio unificato ed un account amministrativo nei domini da dismettere. Tale account potrà essere utilizzato da remoto anche a termine della esecuzione sul territorio dei lavori fino a completamento delle procedure.

A riconoscimento di servizio ultimato l'account amministrativo verrà dismesso.

Dal momento che il servizio oggetto dell'affidamento implica il blocco delle attività dipartimentali o comunque una loro forte compromissione, il fornitore si impegna ad eseguire e completare nella loro piena funzionalità le attività previste nei tempi come sotto indicati per singolo dipartimento:

- n.1 (una) giornata lavorativa per gli interventi critici lato server (fatto salvo il sistema WSUS non ritenuto critico). Per riconosciuti impedimenti di natura tecnica, è consentita una seconda giornata di lavoro;
- n.4 (quattro) giornate lavorative consecutive per sostituzione progressiva switch, e interventi lato client nel corso dei quali saranno effettuate messe in esercizio dei client progressivamente trattati.

Gli interventi complessivi non potranno comunque superare n.5 (cinque) giorni sul territorio per ciascun dipartimento.

Al termine delle giornate sopra indicate il dipartimento deve essere in grado di riprendere in pieno le sue funzioni; quindi i nuovi server dovranno essere in completo esercizio con i servizi di dominio attivi ed i profili utenti completamente migrati, tutte le postazioni client dovranno essere utilizzabili, gli switch operativi, le stampanti configurate ed accessibili tramite printer server, i

servizi di file server accessibili, il sistema di BACKUP collaudato e funzionante, il sistema WSUS operativo.

I due dipartimenti in oggetto dovranno necessariamente essere trattati in due fasi separate.

7) Condizioni di affidabilità

Al fine di garantirsi l'adeguatezza del servizio offerto, ARPAM richiede che il fornitore sia in possesso di adeguate condizioni di affidabilità.

In particolare, per la configurazione del server, del dominio e della rete si richiede che il tecnico senior di riferimento indicato dal fornitore e che eseguirà le prestazioni sia in possesso della certificazione Microsoft (MSCA) Windows Server 2016.

Il tecnico senior certificato è tenuto ad essere presente almeno durante le fasi di gestione del server, degli switch, del backup e della unificazione del dominio e dovrà impostare le procedure di migrazione account. Qualora il tecnico senior certificato non fosse presente durante gli interventi sui client, egli deve essere immediatamente reperibile ed in grado di intervenire da remoto o recarsi sul posto entro un'ora in caso di problemi.

RESPONSABILE DEL TRATTAMENTO DEI DATI

Con la firma del contratto, la ditta appaltatrice viene designata quale Responsabile del trattamento dei dati in relazione alla fase di esecuzione del contratto medesimo. Con separato contratto, il cui schema viene pubblicato in allegato al presente documento e che la ditta aggiudicataria si impegna a restituire sottoscritto prima della stipula, il titolare e l'appaltatore provvederanno a disciplinare compiti, funzioni, ruoli e responsabilità in ordine al trattamento dei dati. In ogni caso, in relazione alla fase di esecuzione del contratto l'appaltatore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi compresi i dati sensibili e giudiziari, nonché quelli che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma, fatto salvo il caso in cui sia strettamente necessario per l'esecuzione del contratto trasmettere dati a terzi, e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del contratto.

DATA DI ULTIMAZIONE DEL SERVIZIO

Il servizio dovrà essere ultimato entro il 15 dicembre 2020, salvo diverso ed ulteriore termine assegnato dal Direttore dell'esecuzione.