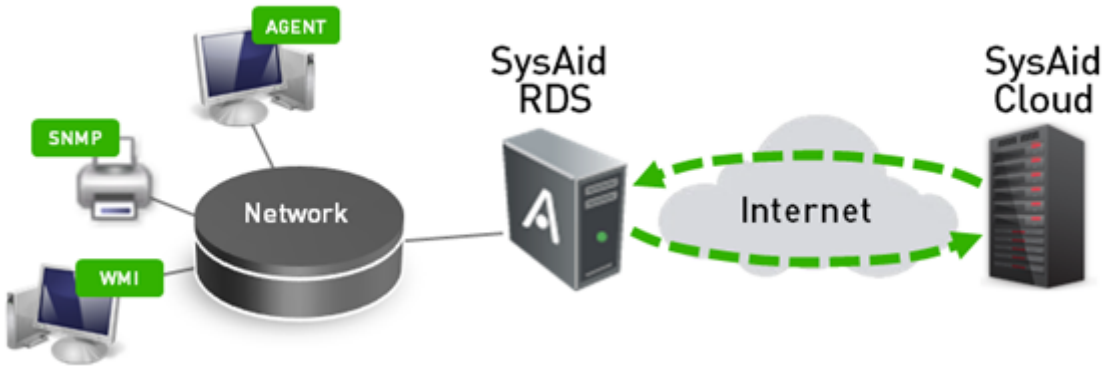
SysAid Cloud: Requisiti & Best Practice per l'Attivazione

SysAid rel. 22 – Gennaio 2022

1. Introduzione

Scopo di questo documento è di fornire i requisiti necessari e le best practice per supportare le organizzazioni nell'uso corretto di SysAid Cloud.

La seguente immagine mostra l'architettura tipica di SysAid Cloud.



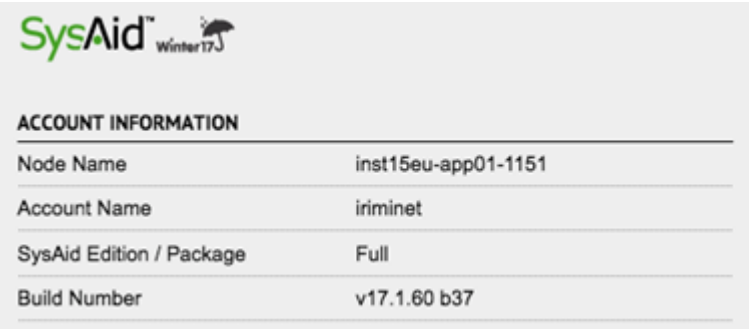
2. Accesso alla rete

Per consentire le comunicazioni tra SysAid Cloud e i tuoi servizi aziendali per le finalità di integrazione email, LDAP, etc., deve essere garantita l'accesso alla tua rete aziendale da parte del servizio cloud.

a. Identificare l'istanza cloud

Per prima cosa devi identificare l'istanza cloud che ospita il tuo account SysAid:

1. Accedi a SysAid
2. Clicca sul tuo nome in alto a destra e accede alla sezione About/Informazioni
3. Controlla il campo Node Name



Nel caso riportato nell'immagine:

- **inst15** è il numero identificativo dell'istanza cloud che ospita il tuo account
- **eu** è l'identificativo geografico del datacenter (Europe)

b. Abilitare le comunicazioni

Una volta identificato l'ambiente cloud, assicurati di aprire il tuo firewall per i seguenti indirizzi IP che corrispondono ai nostri server SysAid.

DATACENTER PRIMARIO	INDIRIZZI IP
Europe	18.203.193.231 54.194.120.197 54.194.152.168 54.194.82.162 54.229.87.79 54.229.87.34 34.249.83.117 63.35.129.150 63.35.31.184 54.229.87.39 45.136.240.0/22 2a0e:9dc0:15::/48 54.194.126.199 54.72.51.192 54.72.88.174 54.72.134.87

Se il tuo account SysAid non si trova sul datacenter Europe, contattaci

In base alle integrazioni che intendi configurare, occorre dare accesso alla tua rete attraverso le seguenti porte:

INTEGRAZIONE	PORTA NON SICURA	PORTA SSL
IMAP	143 TCP	993
POP3	110 TCP	995
LDAP*	389 TCP	636
SSO (NTLM)	139 e 445	

* SysAid Cloud può importare gli utenti dal tuo sistema LDAP.

Ci sono due modi per abilitare le comunicazioni tra il server LDAP e SysAid Cloud:

- **(Opzione consigliata)** Installare **SysAid RDS** in locale e utilizzarlo come gateway delle comunicazioni tra server LDAP e SysAid Cloud. Guarda i requisiti di SysAid RDS (punto 3.a)

  Oppure

- Attivare l'accesso al tuo server LDAP dagli indirizzi IP indicati sopra (punto 2.b) tramite la porta configurata sul tuo firewall

3. Requisiti

a. SysAid Remote Discovery

Per utilizzare le capacità di integrazione LDAP e di Network Discovery in sedi remote, SysAid Cloud raccomanda di installare SysAid Remote Discovery Service (RDS). Si tratta di un servizio proxy da installare su una macchina nella rete locale che si occupa di effettuare i processi di monitoring, network discovery, e integrazione LDAP per poi comunicare i dati acquisiti al SysAid Cloud.

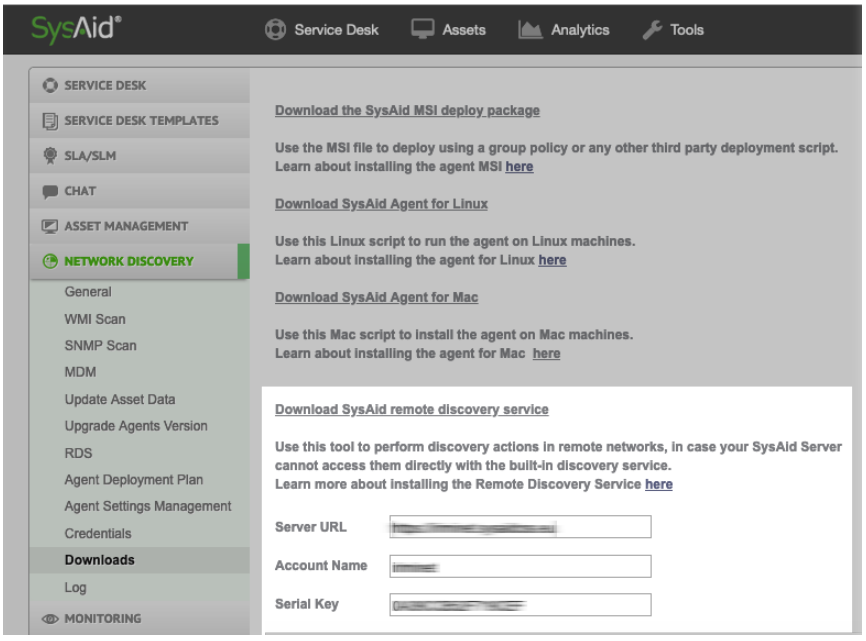
Utilizzare SysAid RDS assicura che tutto il traffico di rete generato durante il network discovery e il monitoraggio resti in locale riducendo il traffico di rete e aumentandone l'affidabilità.

COMPONENTE	REQUISITI	
	MINIMI	RACCOMANDATI
Computer e processore	Dual-Core	Quad-Core
RAM	4 GB	8 GB
Spazio HD Libero	10 GB	
Sistema Operativo (32-bit o 64-bit)	Windows* 11, 10. 8, 7, Windows Server 2008, Server 2008 R2, Server 2012, Windows Server 2012 R2, Server 2016, Server 2019, Server 2022	
Connessione di rete	Deve poter comunicare con il SysAid Server	
Rapporto RDS/Asset	Si raccomanda 1 SysAid RDS: • Ogni 500 asset per sede locale • Ogni 20 asset per sede remota	

* Richiede .NET Framework 3.5 SP 1 o superiore

Se intendi implementare le funzioni di Patch Management di SysAid, verifica i requisiti aggiuntivi (punto 3.c).

Per scaricare SysAid RDS, accedi al tuo SysAid in Settings > Network Discovery > Downloads.



b. SysAid Agent (client-side)

COMPONENTE	REQUISITI RACCOMANDATI
Computer e processore	1.5 GHz
RAM	512 MB
Spazio HD	50 MB *
Utilizzo RAM	20 MB
Sistema Operativo* (32-bit o 64-bit)	• Windows** 11, 10, 8, 7, Vista, Windows Server 2022, 2019, 2016, 2012, 2008 • Linux *** • Mac OS X 10.11 e superiore • Unix, IBM AIX, FreeBSD, Solaris, HP-UX ****

* Sono richiesti 1.5 GB aggiuntivi per le funzioni di Patch Management

** Richiede Framework .NET SP1 3.5 o superiore per le funzioni di network discovery

Il servizio Remote Registry deve essere attivo e in modalità di avvio automatico.

*** Solo per le capacità di network discovery (il pacchetto LSHV deve essere B.02.16)

**** Attraverso uno strumento di terze parti (contattaci per maggiori informazioni)

c. SysAid Patch Management

I seguenti requisiti si riferiscono al SysAid RDS e sono aggiuntivi rispetto ai requisiti riportati nelle tabelle precedenti.

COMPONENTE	REQUISITI AGGIUNTIVI	
	MINIMI	**RACCOMANDATI**
RAM	4 GB	8 GB
Spazio HD	10 GB	20 GB
Banda di connessione	1544 kbps	
Porta	1070	

d. Integrazioni

COMPONENTE	REQUISITI RACCOMANDATI / PROTOCOLLI SUPPORTATI
Outbound Email	SMTP/S
Inbound Email	• OAuth2.0 (O365 e Google) • POP3/S • IMAP/S • EWS / Microsoft Basic (Microsoft Exchange e O365 • MAPI (Microsoft Exchange, solo rete locale)
LDAP	• Microsoft Active Directory (con configuration wizard) • Qualsiasi directory LDAP-based (es. Open LDAP) • Integrazione con Azure AD* (via Marketplace)
API	Richiede un ambiente di sviluppo integrato (IDE) che supporti la generazione di oggetti da file .wsdl

SMS	• Account HTTP(S) con gateway SMS (Clickatell, Red Oxygen, Office Core/SMSCenter) • Qualsiasi altro gateway che supporti HTTP(S) API (contattaci per maggiori informazioni)
SSO *	• Microsoft ADFS • Central Authentication Services (CAS) • Integrazioni terze parti (Google Apps, Office 365, OpenAM, OneLogin, Shiboletth)
Exchange (Calendar)	Supportato con protocollo MAPI solo per Microsoft Exchange
Office365 (Calendar)	Supportato con protocollo EWS
Report editing	Richiede iReport versione 3.7.6

* Richiede SysAid edizione ITSM

e. User Interface

COMPONENTE	REQUISITI / BROWSER SUPPORTATI
Utenti Finali *	Internet Explorer 11** o superiore, Edge, Firefox, Chrome, Safari***
Amministratori *	Internet Explorer 11** o superiore, Edge, Firefox, Chrome, Safari***
Controllo remoto (RCG), My Desktop *	Richiede un browser compatibile HTML5 (IE 11, Edge***, Firefox***, Chrome***)
Risoluzione Schermo	1280 x 1024 o superiore

* Estensioni o componenti del browser per il blocco di finestre e pop-up (es. AdBlock) possono interferire con le capacità di SysAid. Si consiglia di aggiungere l'URL di SysAid ai filtri di esclusione dell'estensione o componente.

** Versioni precedenti del browser potrebbero non supportare tutte le capacità delle release attuali di SysAid

*** Le funzionalità base sono supportate

f. App mobile

Per attivare l'accesso alla web app, contattaci

COMPONENTE	REQUISITI
Web App	Qualsiasi dispositivo
SysAid Release	21.4 o superiore
Licenza	€

4. Requisiti Specifici

In questa sezione sono riportati le specifiche dei requisiti di sistema e di infrastruttura per i principali moduli e funzionalità di SysAid.

I requisiti di funzionamento per i moduli non presenti in questo documento (Password Services, BI Analytics, integrazione con Jira Software, Automate Joe, etc.) sono consultabili sulla guida online.

a) Agent deployment

COMPONENTE	REQUISITI
Credenziali	Il deployment del SysAid Agent richiede le credenziali di amministratore di dominio: Settings > Asset Management > Credentials Management
Porte	Per eseguire il deployment, tra SysAid Server/RDS e le macchine target, devono essere aperte le seguenti porte: • CP 139, TCP 445, UDP 137, UDP 138 e UDP 8193 Per consentire le comunicazioni tra SysAid Agent e SysAid Server/RDS, deve restare aperta la porta 8193
Servizi in esecuzione	Su ogni macchina target, devono essere attivi i seguenti servizi: • Server (in esecuzione per default) • Remote Procedure Call (RPC, in esecuzione per default) • Remote Registry
Antivirus	I sistemi antivirus devono prevedere le seguenti esclusioni: SysAid Server • ..\SysAidServer* e comprese tutte le subfolders RDS: • ..\SysaidRemoteDiscovery* comprese tutte le subfolders Processi: • java.exe • InstallAgent.exe • SysAidWorker.exe • NetworkDiscovery.exe • Inssatt.exe • mantle.exe • Wrapper.exe • SysAidSM.exe • httpd.exe Macchine target / SysAid Agent: • ..\SysAidAgent* e comprese tutte le subfolders Macchine target / Processi SysAid Agent: • C:\Program Files\SysAid\SysAidSM.exe • C:\Program Files\SysAid\SysAidWorker.exe
Alias DNS	Il metodo ottimale per connettersi all'applicativo è di utilizzare un alias DNS (CNAME) per risolvere l'indirizzo IP del SysAid Server. In questo modo, nel caso in cui sia necessario spostare SysAid su un'altra macchina, l'operazione può essere svolta facilmente evitando il ri-deploy degli agent.

b) Remote Control Gateway

Il Remote Control Gateway (RCG) è il metodo di controllo remoto in-browser, nativo di SysAid.

COMPONENTE	REQUISITI
Browser	Supporto HTML5
Porte	Le porte 443 e 8443 del server RCG (di default SysAid Server) devono essere accessibile dal computer che avvia il controllo remoto e il computer target.

c) TeamViewer Embedded Service

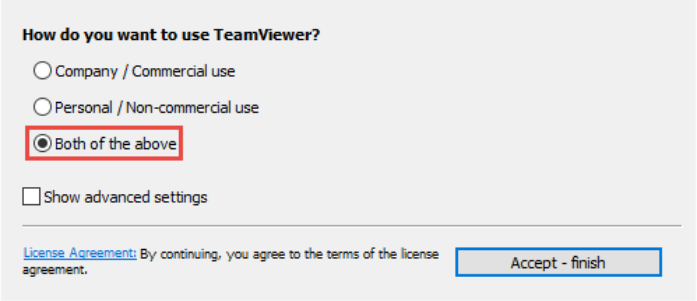
SysAid TeamViewer Embedded Service fornisce le capacità di controllo remoto per mezzo dell'integrazione con TeamViewer; in questo modo puoi avviare una sessione da remoto direttamente dal service record con un utente, bypassando eventuali limitazioni UAC e senza necessità del SysAid Agent.

SysAid TeamViewer Embedded Service consente anche il controllo da remoto di asset non presidiati - in questo caso per aprire e chiudere le connessioni in sicurezza, è richiesto il SysAid Agent sulla macchina target.

COMPONENTE	REQUISITI
Network	• Il computer che avvia la sessione e la macchina target devono poter accedere a internet, all'URL di TeamViewer
TeamViewer Server	• Tutti i server TeamViewer devono essere raggiungibili. Il modo più semplice è lasciare aperta la porta 5938 (TCP) a tutte le connessioni in uscita. Altrimenti puoi aggiungere Teamviewer.com alla tua whitelist.
SysAid URL	• L'URL di SysAid deve essere accessibile dall'esterno rispetto alla rete aziendale • Non è possibile utilizzare l'indirizzo IP del server
SysAid Release	17.2.40 o superiore
SysAid On-Premise	Assicurarsi che SysAid Server abbia accesso a SysAid Gateway raggiungibile a questo URL: https://gateway.sysaid.com
Permessi	Solo gli amministratori autorizzati possono avviare sessioni di controllo remoto (vedi i permessi per Amministratori)

Per evitare di scaricare e installare TeamViewer.exe per ogni sessione, raccomandiamo di:

- Installare TeamViewer sulla macchina dell'amministratore prima di iniziare ad utilizzare TeamViewer Embedded Service;
- Durante l'installazione selezionare che si intende utilizzare TeamViewer sia per scopi personali che commerciali (Both of the above)



5. Network discovery: banda e risorse

SysAid integra capacità complete di asset management: è in grado di tracciare computer, stampanti, server, switch, router e molto altro. Uno dei vantaggi principali di SysAid Asset Management è quello di offrire diversi metodi di discovery degli asset connessi in rete.

SysAid può effettuare i seguenti tipi di scansione:

- WMI
- SNMP
- Agent deployment

Scansione WMI

SysAid permette di rilevare i computer in rete con sistema operativo Windows attraverso la scansione WMI.
Questo tipo di scansione non richiede l'installazione di agent e restituisce un'istantanea dei computer in rete e delle loro componenti.

La scansione WMI può essere effettuata in due modi: per dominio o per range di IP. I processi di scansione possono essere pianificati ad intervalli specifici.

- Ogni asset individuato via scansione WMI crea un dataset di circa **100 KB**

Scansione SNMP

SysAid supporta la scansione SNMP per la gestione automatica dell'inventario dei dispositivi SNMP. Importare un dispositivo SNMP in SysAid permette di: avere informazioni sugli asset SNMP costantemente aggiornate; di scrivere sui dispositivi SNMP; di ricevere trap SNMP (tramite SysAid Monitoring).

La scansione SNMP viene effettuata per range di IP. Quando un asset viene individuato a seguito di una scansione SNMP, SysAid utilizza il MAC address della prima interfaccia di rete rilevata sul dispositivo come ID dell'asset. La scansione SNMP può essere pianificata per avviarsi in specifici intervalli.

Se la scansione SNMP avviene all'interno della stessa LAN del SysAid Server, la scansione può essere avviata direttamente dal SysAid Server. Se la scansione deve essere eseguita su un'altra rete o in presenza di firewall, è necessario indirizzare il processo tramite un SysAid RDS installato nella rete remota.

- Ogni asset individuato via scansione SNMP crea un dataset di circa **5 KB.**

Nel caso in cui la scansione SNMP individui più OID, la dimensione del file potrebbe aumentare

Agent deployment

Il SysAid Agent è un'applicazione installata sugli asset che lavora in background e che abilita, oltre alle capacità di asset inventory automatico, anche il controllo remoto, il monitoring di rete e server, etc.

Il deployment degli agent può essere eseguito via:

- Network Discovery (Agent Deployment Plan)
- SysAid Administrators tool
- MSI deployment package
- Network login script

- Asset importati tramite scansione WMI

Gli agent installati sugli asset comunicano con il SysAidServer oppure con il Remote Discovery Service a seconda delle specifiche configurazioni della tua installazione di SysAid. Nel caso di SysAid Cloud, l'RDS deve essere installato come prerequisito per consentire la comunicazione con il server in cloud.

1. Installazione: **50 MB** (vedi punto c)
2. Una volta installato, il SysAid Agent genera un file .xml (**100 KB**) e lo invia al SysAid Server/RDS
3. L'agent si connette SysAid Server/RDS ogni 30 secondi (valore di default).
   Il polling richiede **0,005KB/poll**.

In base alle condizioni sopra citate, un singolo asset produce traffico pari a **0,6 KB/ora**.

Esempio: con 2000 asset connessi ad un RDS, il consumo di banda degli agent è pari a **1,2 MB/ora**.

6. Ambiente di test

Puoi richiedere un ambiente di test (On-Prem o Cloud) come servizio opzionale per scopi come:

- Sviluppare script personalizzati, integrazioni di terze parti o trigger
- Modificare le configurazioni del sistema (es. regole di escalation, regole di routing, ecc)
- Testare qualsiasi cambiamento prima di implementarlo

L'ambiente di test on-prem richiede le stesse risorse di un ambiente di produzione on-premise (scarica i requisiti on-premise).

Per impedire interferenze con l'installazione di produzione, è necessario che alcune funzionalità siano disabilitate :

- l'integrazione di email in entrata e in uscita
- il deploy degli agent e le scansione WMI/SNMP
- qualsiasi regola o impostazione che possa influire sull'ambiente di produzione

7. Risorse & assistenza

- Requisiti di sistema: http://www.sysaid.com/support/system-requirements
- VMware best practices: http://www.vmware.com/resources/techresources/1087
- Guida Online SysAid: http://www.sysaid.com/resources/documentation

Per richiedere assistenza tecnica

- Centro di Supporto: https://support.irimi.it/
- Telefono:I +39 0445 1948007